5G End to End

5G Introduction

Module 1

- Introduction to 5G
- 5G Requirements

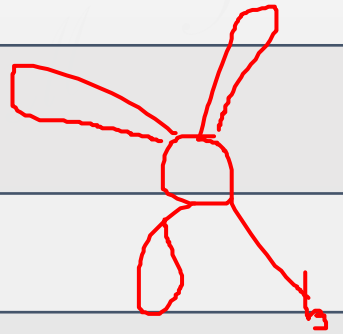
Introduction to 5G

What is 5G?

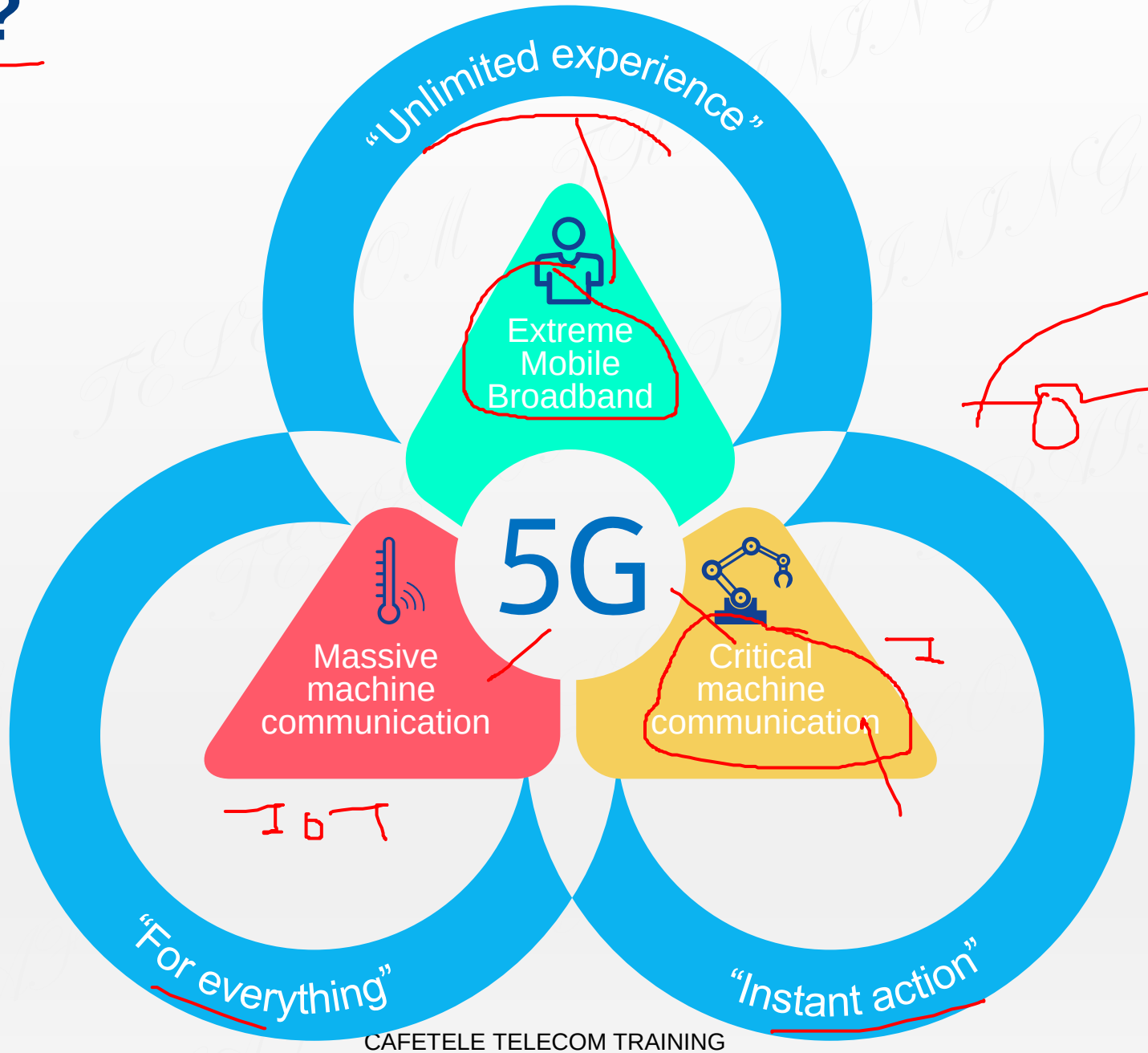
5G has been introduced within the release 15 version of the 3GPP specifications, whereas 4G was introduced within release 8.

5G has been specified based upon the requirements of the following use cases:

- Enhanced Mobile Broadband (eMBB)
- Ultra Reliable and Low Latency Communications (URLLC)
- Massive Machine Type Communications (mMTC)



What 5G is ?


“Unlimited experience”
Extreme Mobile Broadband
5G
Massive machine communication
Critical machine communication
“For everything”
“Instant action”

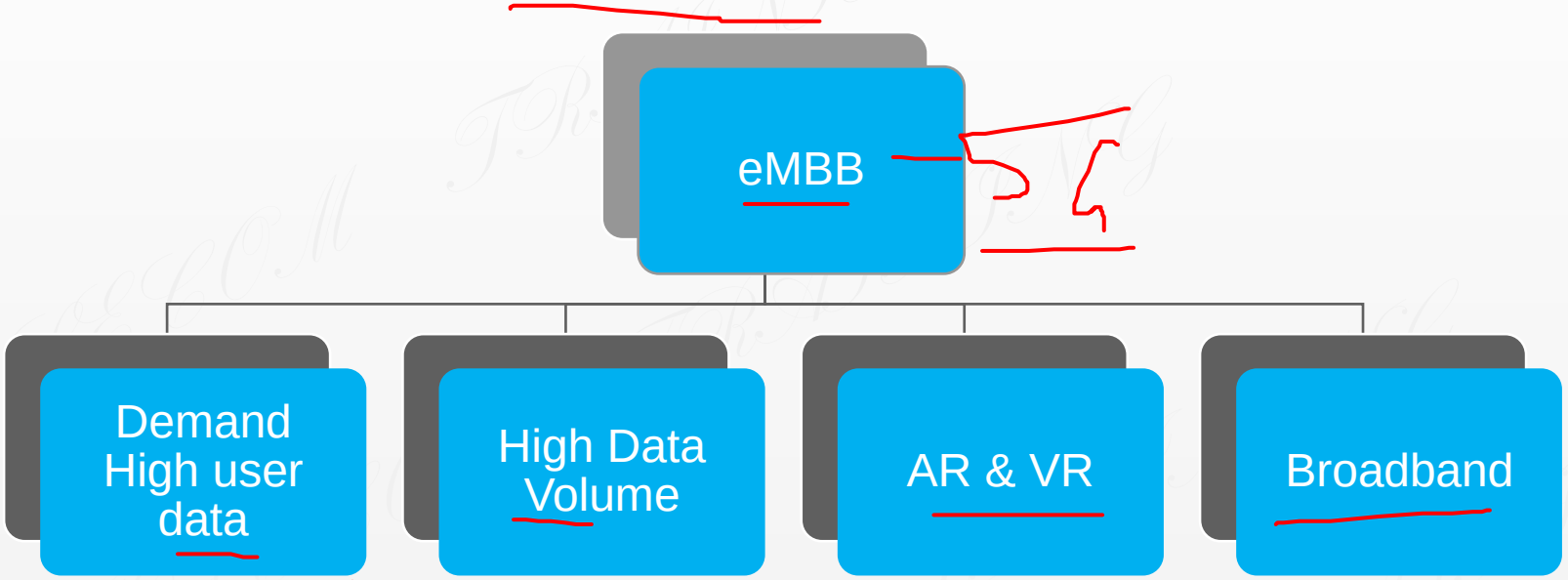
Future network requirements

End-to-end 5G builds upon existing 4G LTE deployments

Evolution of communication: from 2G to 5G

	2G GSM	2.7G EDGE	3G WCDMA	3.5 HSPA, HSPA+	4G LTE	4G LTE-Advanced	4,5G LTE-A Pro	5G
3GPP Release	Rel. 97	Rel. 98	Rel. 99	Rel. 5,6,7	Rel. 8,9	Rel. 10,11,12	Rel. 13,14	Rel 15, 16
Use case	Digital voice & messaging Digital fidelity cellular phones	Enhanced 2G Higher data rates	Voice, Data & Video Signals Video Telephony / Internet surfing	Enhanced 3G Higher data rates	Data and Voice over IP Wireless broadband	Enhanced 4G Higher peak rates	4G Evolution towards 5G +IoT and Public safety	eMBB, critical MTC, massive MTC 4th industrial revolution
Channel access	TDMA/FDMA	TDMA/FDMA	WCDMA	WCDMA	OFDMA	OFDMA	OFDMA	Modified OFDMA
Bandwidth	200 kHz	200 kHz	5 MHz	5 MHz	20 MHz	100 MHz	640 MHz	Up to 2 GHz
Service	CS	CS/PS	CS/PS	PS	PS	PS	PS	PS
Architecture	Controller	Controller	Controller	Controller	Distributed	HetNet	Cloud	Cloud, co-existence, slicing
DL speed	40 Kbps	500 Kbps	384 kbps	14-84 Mbps	150-300 Mbps	1 Gbps	3 Gbps	>10 Gbps
Latency	~500 ms	~300 ms	~150ms	~50 ms	~10ms	~10ms	~5ms	<1ms

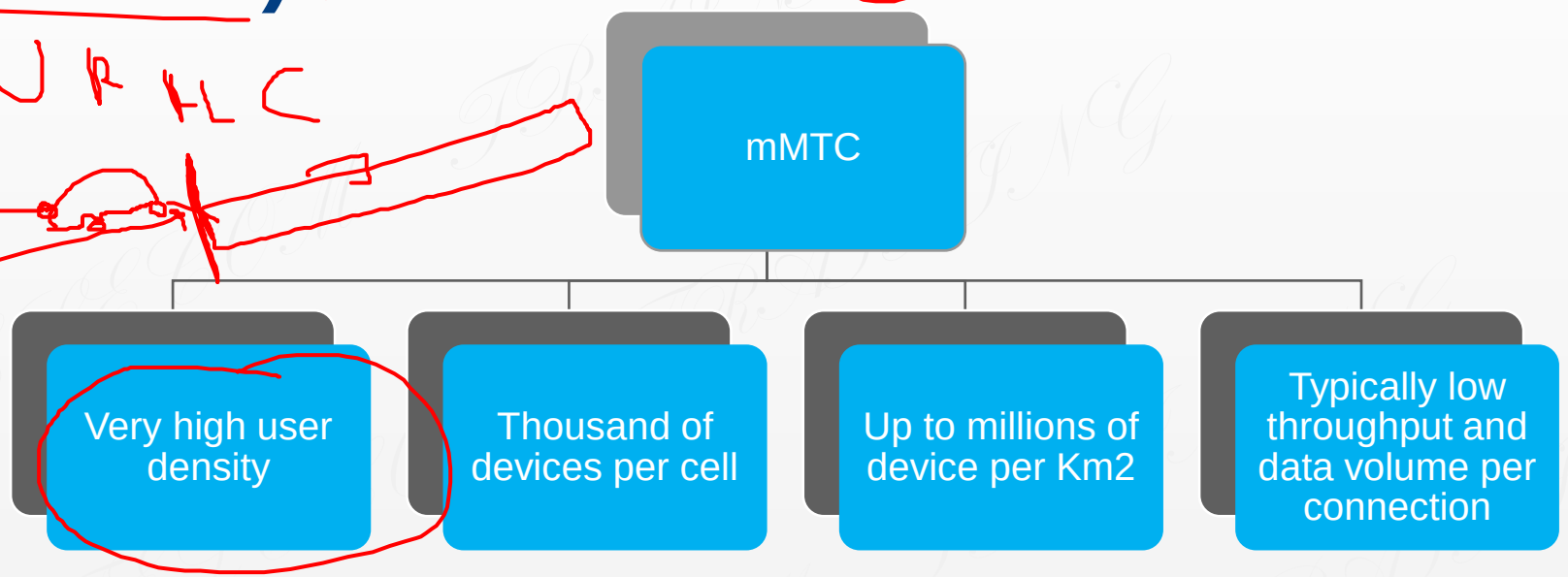
Enhanced Mobile Broadband(eMBB)



Use Cases

Category	Application	Application type	Peak Throughput	Avg Thp	Latency
Mobile Entertainment	8K Video UHD Streaming	eMBB	80 Mbps	30 Mbps	< 200 ms
	360 Video next gen 90 FPS	eMBB+URLCC	200 Mbps	50 Mbps	1-2 ms
	Retinal VR	eMBB+URLCC	300 Mbps	100 Mbps	<5 ms
	AR	eMBB+URLCC	<4 Gbps	700 M- 1Gbps	<10 ms
	Mobile TV	eMBB	50 Mbps	10 Mbps	<200 ms
Mobile Broadband	Broadband service	eMBB	200 Mbps		<200 ms

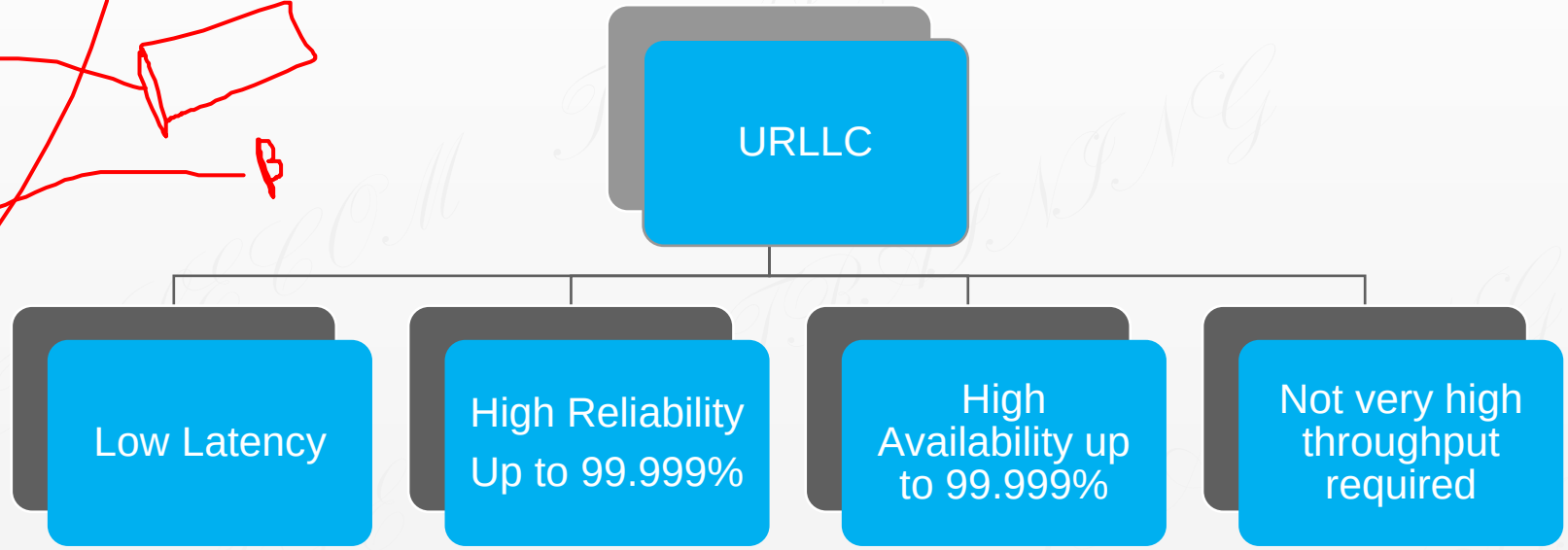
Massive Machine Type Communication(mMTC)



Use Cases

Category	Application	Application type	Peak Throughput	Avg Thp	Latency
IOT	Sensor Network	mMTC	400 Kbps	100 Kbps	NA
	Factory Automation	mMTC	10 Mbps	3 Mbps	<10 ms
	Mobile Robots	mMTC	>10 Mbps	3 Mbps	<2 s
Smart Cities	Smart Parking	mMTC	100 Kbps	<50 Kbps	sec
V2X	Road Warning	mMTC	2mbps	<500 Kbps	<10 ms

Ultra Reliable Low Latency Communication



Use Cases

Category	Application	Application type	Peak Throughput	Avg Thp	Latency
IOT	Tactile Internet	uRLLC	Kbps	100 Kbps	<1 ms
Smart Grid	Power Distribution Network	uRLLC	50 Mbps	5 Mbps	<50 ms
	Power consumption Point	uRLLC	500 kbps	50 Kbps	<100 ms
e-Health	Urgent Health Care	uRLLC	<10 Mbps	3 Mbps	10 ms
	Remote health Monitoring	uRLLC	Low	Kbps	sec
	Remote Surgery	uRLLC	100 Mbps	20 Mbps	<10 ms
	Medical weareable	uRLLC	1 Mbps	Kbps	Na
V2X	Vehicle Platooning	uRLLC+mMtc	20 Mbps	2 Mbps	20 Ms
	Collision Avoidance	uRLLC+mMtc	10 Mbps	2Mbps	10 ms

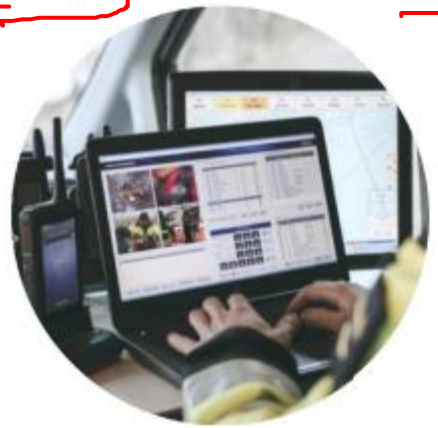
Industries benefiting today and tomorrow

Manufacturing

Transportation

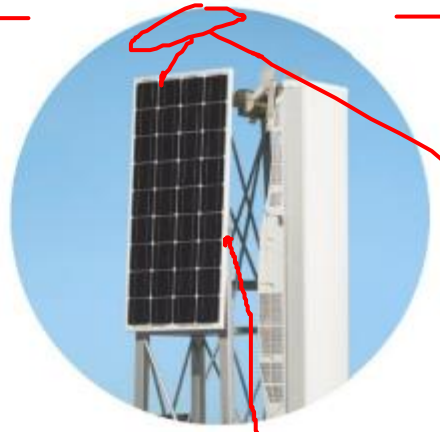
Healthcare

Sports & Entertainment



Public Safety

Mining



Power Industry

3GPP 38-series : Radio technology beyond LTE

TS 38.101	NR; User Equipment (UE) radio transmission and reception
TS 38.104	NR; Base Station (BS) radio transmission and reception
TS 38.133	NR; Requirements for support of radio resource management
TS 38.141	NR; Base Station (BS) conformance testing
TS 38.201	NR; Physical layer; General description
TS 38.202	NR; Physical layer services provided by the physical layer
TS 38.211	NR; Physical channels and modulation
TS 38.212	NR; Multiplexing and channel coding
TS 38.213	NR; Physical layer procedures for control
TS 38.214	NR; Physical layer procedures for data
TS 38.215	NR; Physical layer measurements
TS 38.300	NR; Overall description; Stage-2
TS 38.304	NR; User Equipment (UE) procedures in idle mode
TS 38.306	NR; User Equipment (UE) radio access capabilities
TS 38.307	NR; Requirements on User Equipments (UEs) supporting a release-independent frequency band
TS 38.321	NR; Medium Access Control (MAC) protocol specification
TS 38.322	NR; Radio Link Control (RLC) protocol specification
TS 38.323	NR; Packet Data Convergence Protocol (PDCP) specification
TS 38.331	NR; Radio Resource Control (RRC); Protocol specification
TS 38.401	NR-RAN; Architecture description
TS 38.410	NG-RAN; NG general aspects and principles
TS 38.411	NR-RAN; NG layer 1
TS 38.412	NR-RAN; NG signalling transport
TS 38.413	NR-RAN; NG Application Protocol (NGAP)
TS 38.414	NR-RAN; NG data transport
TS 38.420	NR-RAN; Xn general aspects and principles

TS 38.421	NR-RAN; Xn layer 1
TS 38.422	NR-RAN; Xn signalling transport
TS 38.423	NR-RAN; Xn Application Protocol (XnAP)
TS 38.424	NR-RAN; Xn data transport
TS 38.425	NR-RAN; Xn interface user plane protocol
TR 38.801	Study on new radio access technology: Radio access architecture and interfaces
TR 38.802	Study on new radio access technology Physical layer aspects
TR 38.803	Study on new radio access technology: Radio Frequency (RF) and co-existence aspects
TR 38.804	Study on new radio access technology Radio interface protocol aspects
TR 38.805	Study on new radio access technology; 60 GHz unlicensed spectrum
TR 38.810	Study on test methods for New Radio
TR 38.811	Study on NR to support non-terrestrial networks
TR 38.812	Study on Non-Orthogonal Multiple Access (NOMA) for NR
TR 38.874	NR; Study on integrated access and backhaul
TR 38.889	Study on NR-based access to unlicensed spectrum
TR 38.900	Study on channel model for frequency spectrum above 6 GHz
TR 38.901	Study on channel model for frequencies from 0.5 to 100 GHz
TR 38.912	Study on new radio access technology
TR 38.913	Study on scenarios and requirements for next generation access technologies

Manufacturing

Today

Manufacturing process automation

Tomorrow's use case

Dynamic production control, capacity and agility

Enabled by E2E 5G

Low latency video for immediate control, thousands of sensors with massive connectivity for cloud-based automation

Impact

Revenue from capacity and output

Healthcare

Today

Sharing real-time health data

Tomorrow's use case

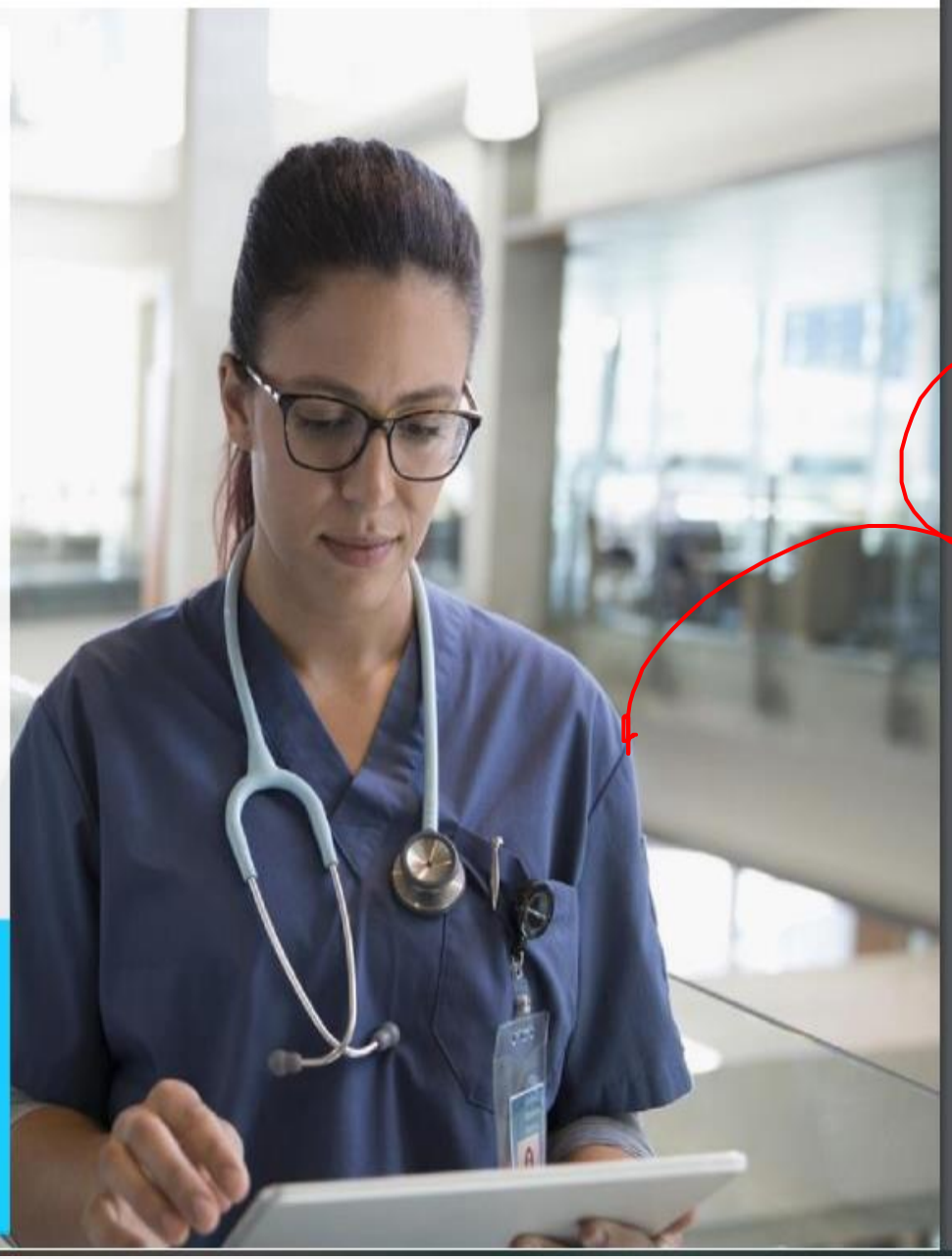
Remotely supported complex health interventions

Enabled by E2E 5G

Low latency network with extreme throughput capacity to deliver crucial imaging and instantaneous medical feedback

Impact

Healthy outcomes from emergency response



Sports & Entertainment

Today

Supporting thousands of smartphones for video, social media

Tomorrow's use case

Immersive device Augmented Reality, with personalized experience

Enabled by E2E 5G

Massive connectivity for multiple video angles, extreme throughput and low latency for high definition Augmented Reality (AR) video for thousands

Impact

Upcharge fees and customer satisfaction

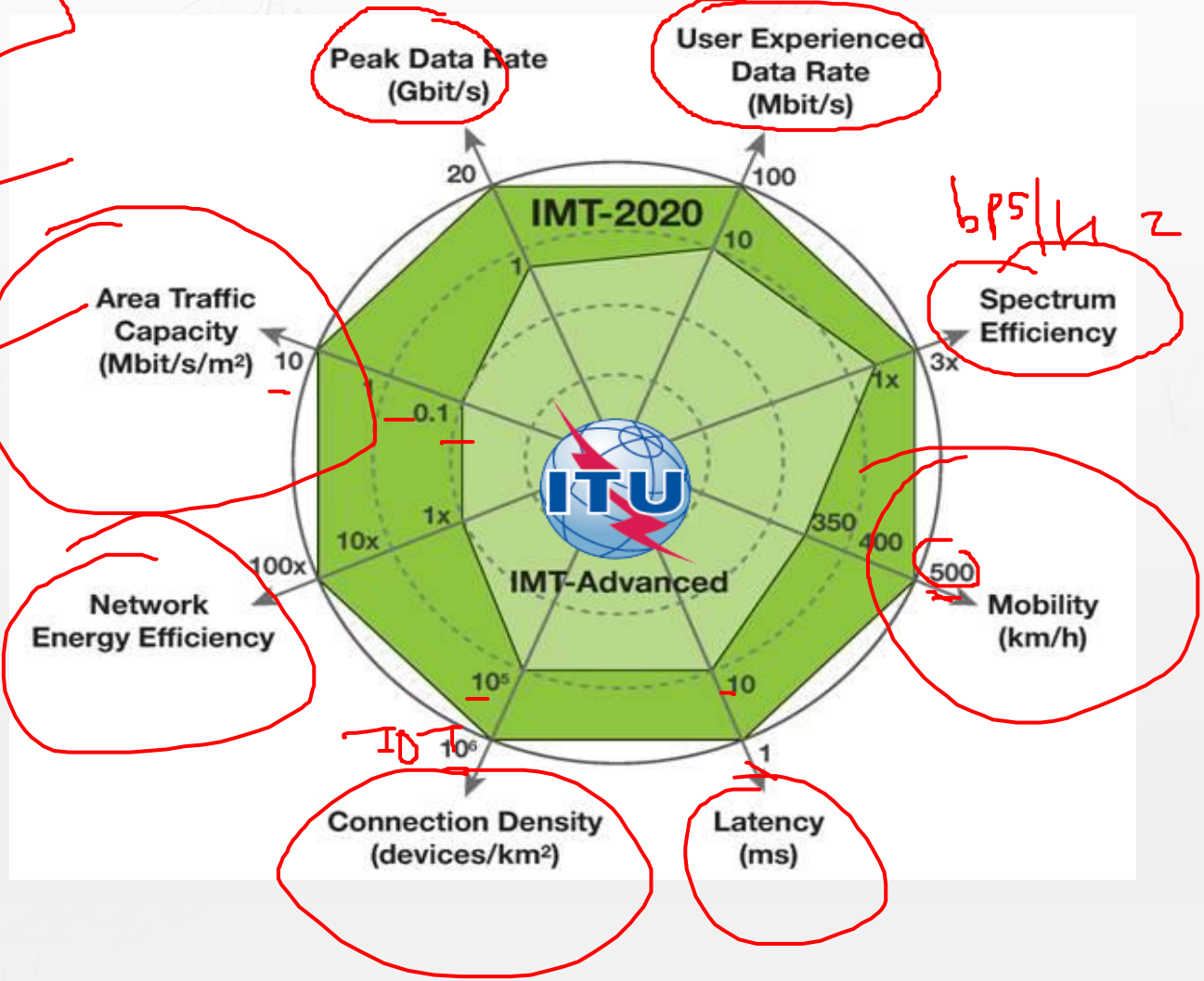
5G Requirements

ITU-R requirements for IMT-2020

ITU-R Recommendation M.2083:

8 key capabilities are identified, at high level, for IMT-2020.

The potential target requirements in this spider chart are only targets for research and investigation and subject to further research.

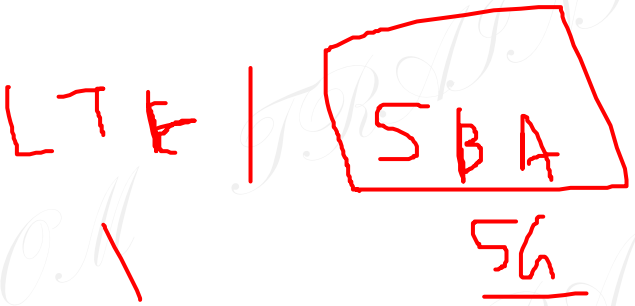


3GPP RAN REQUIREMENT 38.913

Performance Measure	Requirement
Peak data rate	DL: [20 Gbps] UL: [10 Gbps]
Peak spectral efficiency	DL: [30 bps/Hz] UL: [15 bps/Hz]
Spectrum Scalability	Yes
Bandwidth	Reference to IMT-2020
Bandwidth Scalability	Yes
Control plane latency	[10 ms]
UP latency URLLC, one-way	[0,5 ms]
UP latency eMBB, one way	[4ms]
Latency for infrequent small packets	10s / 20byte packet
Mobility interruption time (intra-syst.)	[0 ms]
Mobility	Up to 500 km/h
Inter-system mobility	Yes
Reliability	[1-10^{-5}] in [1ms]

5G NR ARCHITECTURE

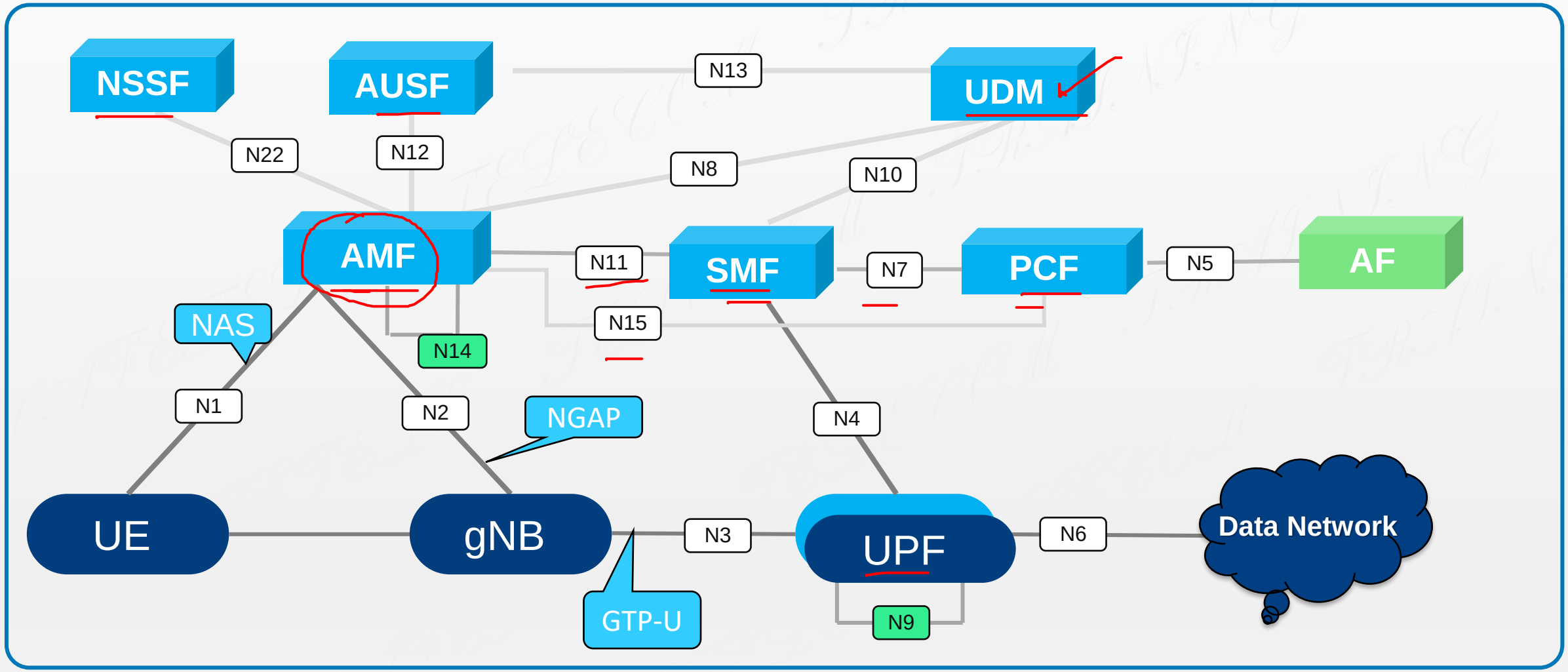
Module 2



- Reference Based Architected
- 5G RAN NSA Networking Introduction
- NSA Network Design and Compare with LTE
- MR DC Architecture
- SA Architecture

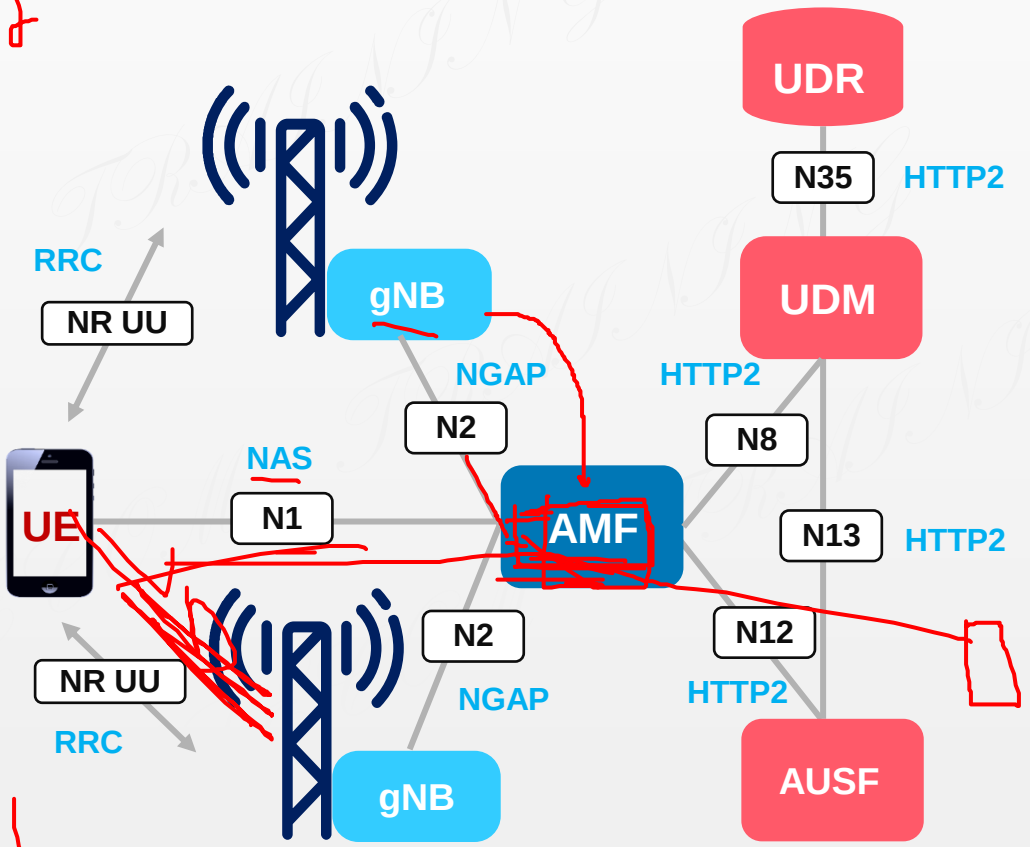
Reference Based Architected

5G System Architecture-Reference Points



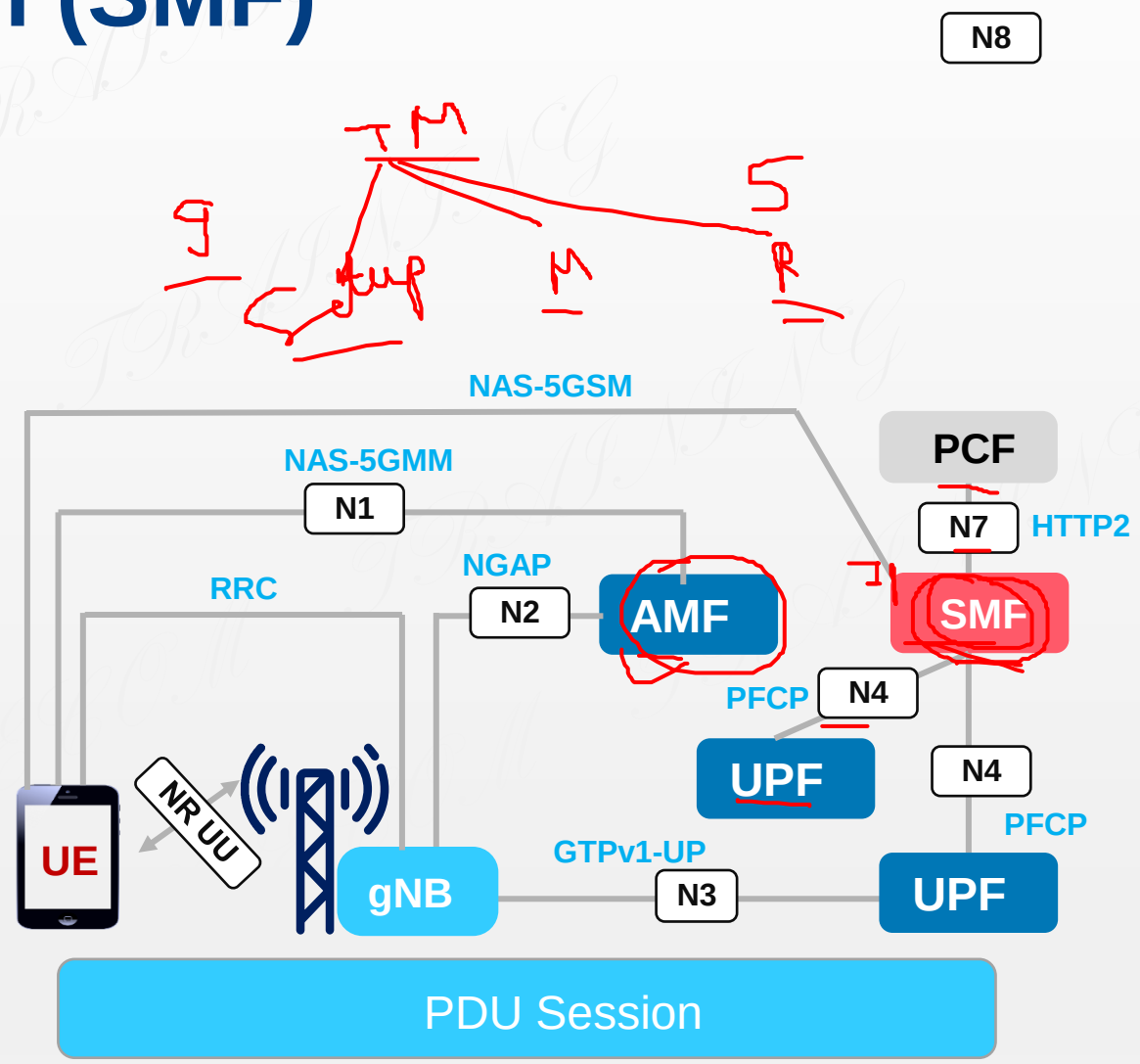
Access and Mobility Management function (AMF)

- Termination of RAN CP interface (N2).
- Termination of NAS (N1)
- NAS ciphering and integrity protection.
- Registration management.
- Mobility Management
- Connection management.
- Reachability management.
- Paging
- Access Authentication.
- Access Authorization.



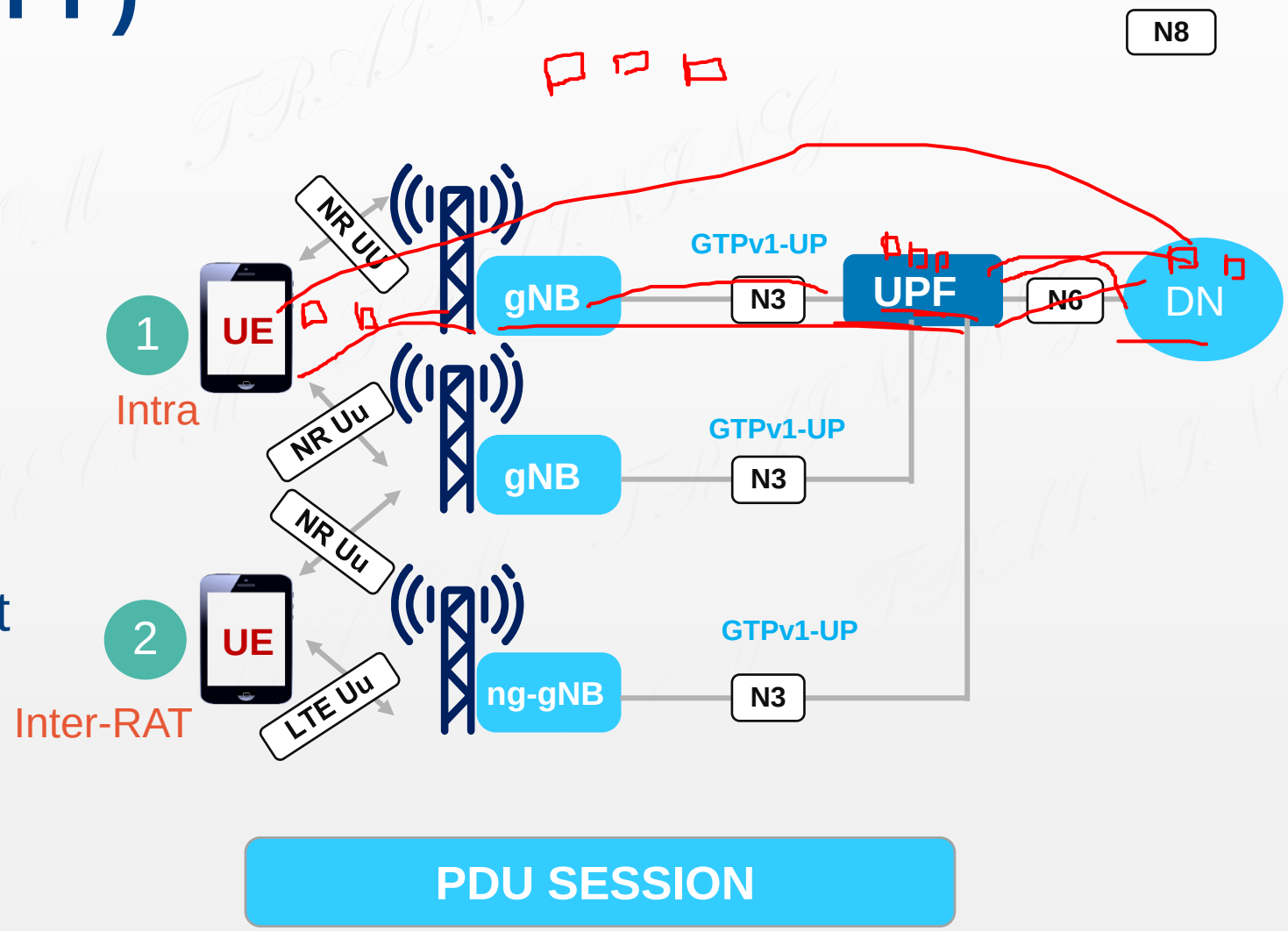
Session Management function (SMF)

- Session Management e.g. Session Establishment, modify and release
- UE IP address allocation (IPV4/IPV6)
- DHCPv4 (server and client) and DHCPv6 (server and client) functions.
- Termination of interfaces towards Policy control function
- Selection and control of UP function
- Termination of SM parts of NAS messages
- Support P-CSCF discovery for IMS services.
- Downlink Data Notification



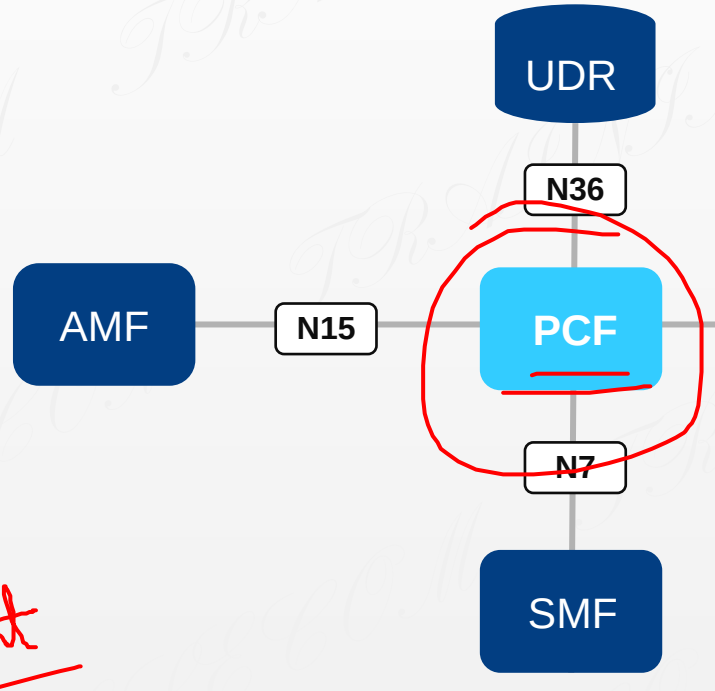
User plane function (UPF)

- Anchor point for Intra-/Inter-RAT mobility
- External PDU Session point of interconnect to Data Network.
- Packet routing & forwarding
- QoS and Policy Rule Enforcement
- Traffic usage reporting
- Data Buffering



Policy Control Function (PCF)

- Policy Decisions
- Policy Rule Distribution
- Access to subscriber information
- Interaction with PCF



Application Function (AF)

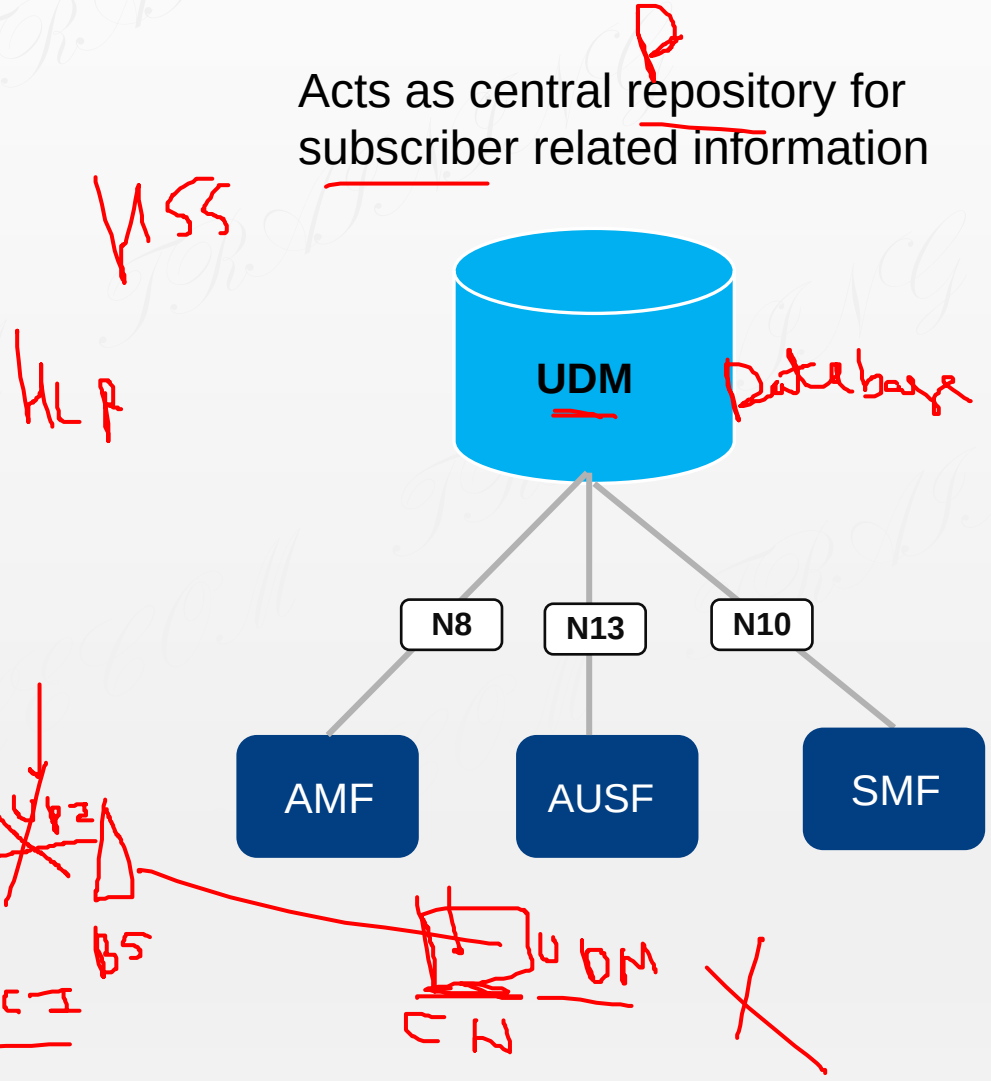
- Prepares session level information to the PCF to support the policy decisions

- Based on operator deployment, Application Functions considered to be trusted by the operator can be allowed to interact directly with relevant Network Functions.

Unified Data Management (UDM)

- Generation of 3GPP AKA Authentication Credentials
  - UDM houses the ARPF for authentication purpose
- User Identification Handling
  - e.g. storage and management of SUPI for each subscriber in the 5G system).
- Support of de-concealment of privacy-protected subscription identifier (SUCI).
- Access authorization based on subscription data
  - e.g. roaming restrictions
- Subscription management.
- Registration/Mobility Management
- UE's Serving NF Registration Management
  - e.g. storing serving AMF for UE, storing serving SMF for UE's PDU Session).
- SMS management.

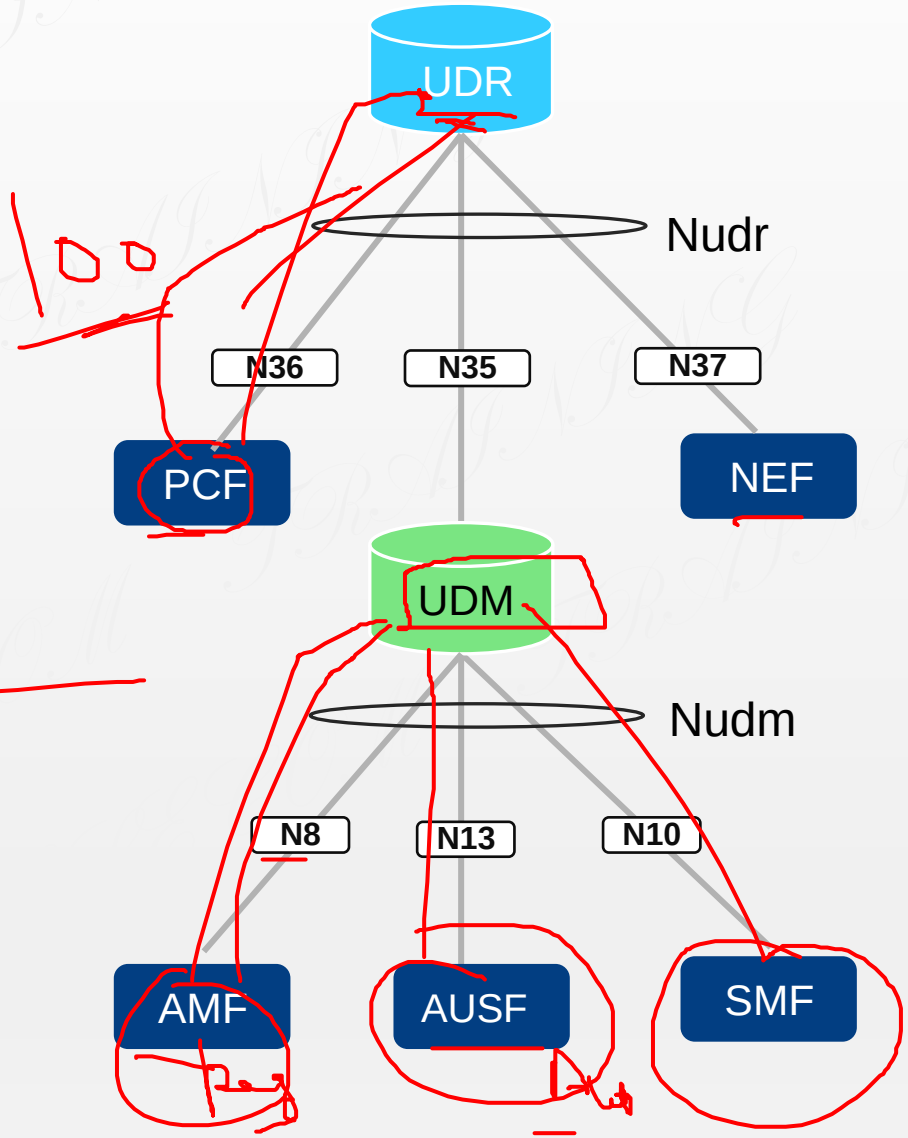
Acts as central repository for subscriber related information



AKA	Authentication and Key Agreement
ARPF	Authentication Repository and Processing Function
SUPI	Subscription Permanent Identifier
SUCI	Subscription Concealed Identifier
SMS	Short Message Service

Unified Data Repository (UDR)

- Storage and retrieval of subscription data by the UDM.
- Storage and retrieval of policy data by the PCF.
- Application data (including PFDs) for application detection
- The Unified Data Repository is located in the same PLMN as the NF service consumers storing in and retrieving data from it using Nudr. Nudr is an intra-PLMN interface.

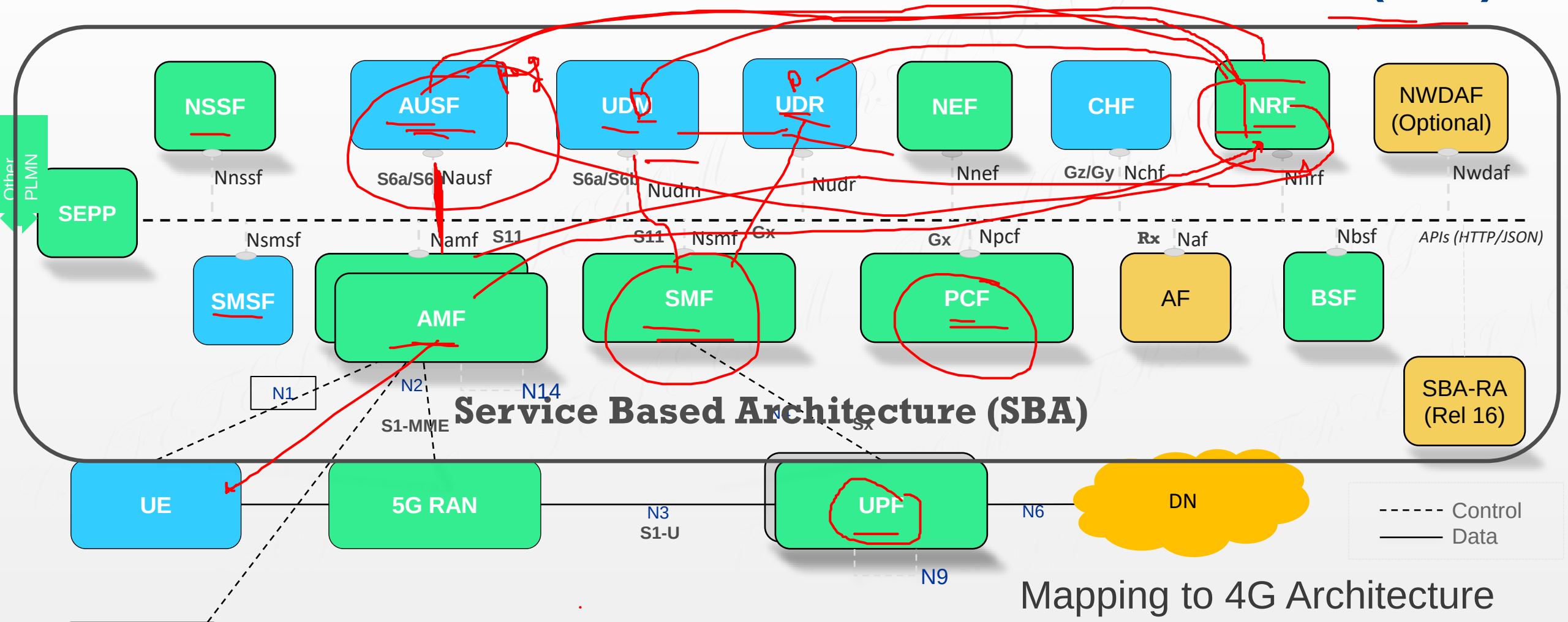


- Nudr SBI supports operations:
  - Read (Reading of Data from UDR)
  - Update (Updating stored data)
  - Delete (Deleting stored data)
- Nudr also support NFs to run subscribe/Notify procedure

SBI Service Base Interface
PFD Packet Flow Description

5G SA Architecture(SBA)

Architecture overview: 5G SA and Service Based Architecture(SBA)



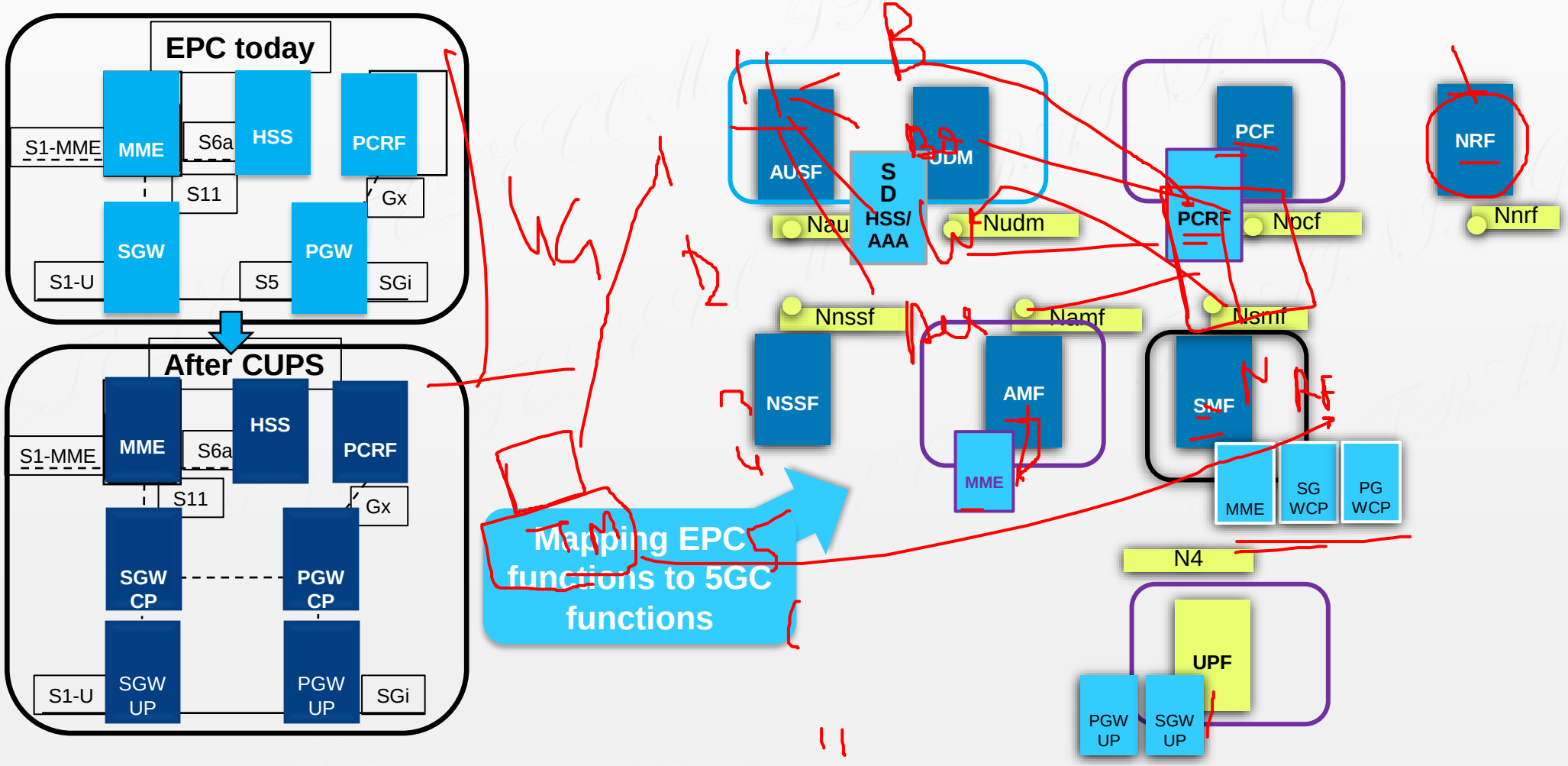
Mapping to 4G Architecture

AF	Application Function
AMF	Access and Mobility Management Function
AUSF	Authentication Server Function
BSF	Binding Support Function
CHF	Charging Function
DN	Data Networks

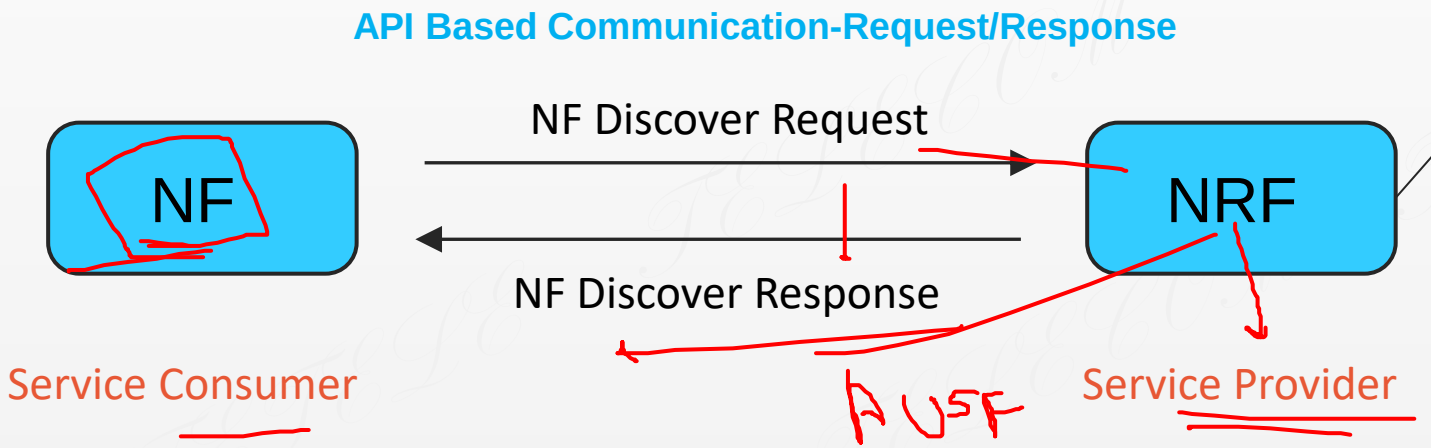
NEF	Network Exposure Function
NRF	NF Repository Function
NSSF	Network Slice Selection Function
NWDAF	Network Data Analytics Function
PCF	Policy Control Function
SMF	Session Management Function

SMSF	SMS Function
SEPP	Security Edge Protection Proxy
(R)AN	(Radio) Access Network
UPF	User Plane Function
UDM	Unified Data Management
UDR	Unified Data Repository

5G Core compared to EPC



Network Repository Function(NRF)



- Maintains the NF profile of available NF instances and their supported services.
- Supports service discovery function. Receive NF Discovery Request from NF instance or SCP, and provides the information of the discovered NF instances (be discovered) to the NF instance
- Maintains the health status of NFs.

NF Profile

- NF instance ID.
- NF type.
- PLMN ID.
- Network Slice related Identifier(s) e.g. S-NSSAI, NSI ID.
- FQDN or IP address of NF.
- NF capacity information.
- NF priority information.

Short Message Service Function(SMSF)

- SMS management subscription data checking and conducting SMS delivery accordingly.
- Relay the SM from UE toward SMS-GMSC/IWMSC/SMS-Router.

Network Slice Selection Function (NSSF)

- Selecting the set of Network Slice instances serving the UE.
- Determining the Allowed NSSAI and, if needed, the mapping to the Subscribed S-NSSAIs;
- Determining the Configured NSSAI and, if needed, the mapping to the Subscribed S-NSSAIs;
- Determining the AMF Set to be used to serve the UE, or, based on configuration, a list of candidate AMF(s), possibly by querying the NRF.

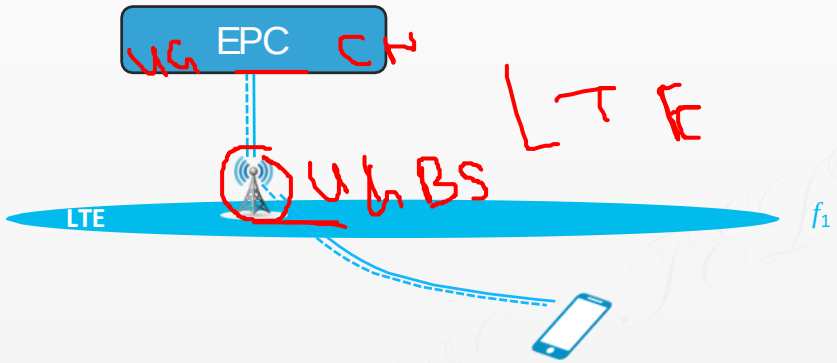
5G-Equipment Identity Register (5G-EIR)

- Check the status of Equipment's identity

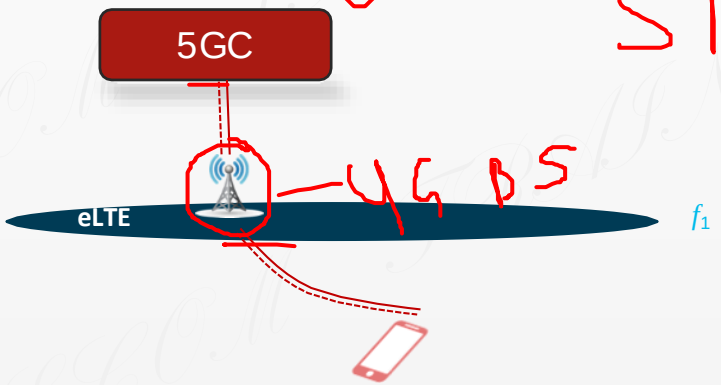
NSA Network Design and Compare with LTE

5G Core Deployment Options

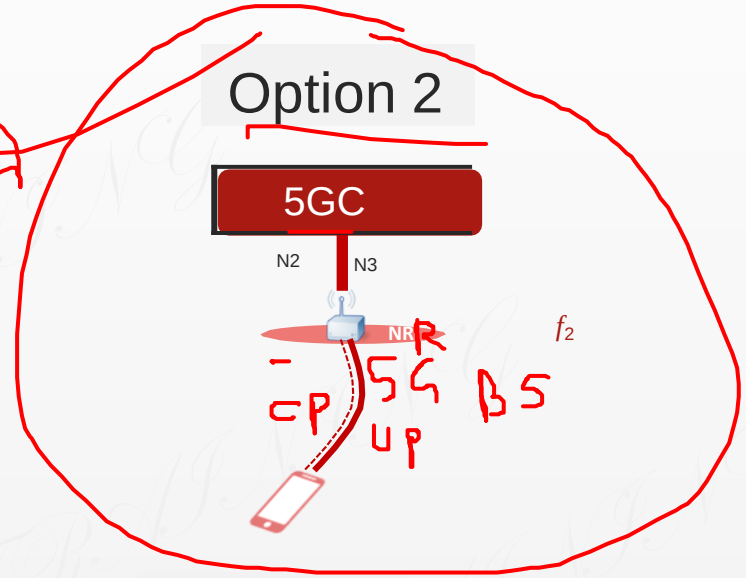
Option 1
(Legacy Networks)



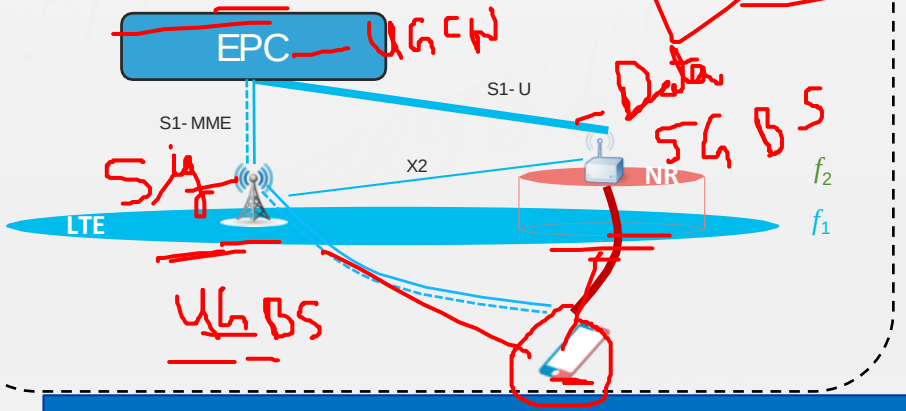
Option 5



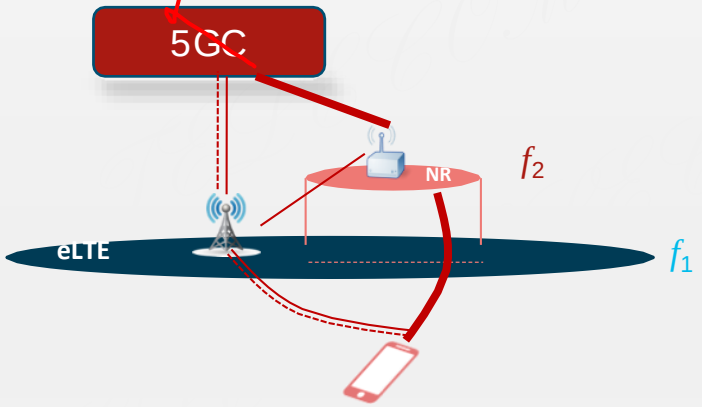
Option 2



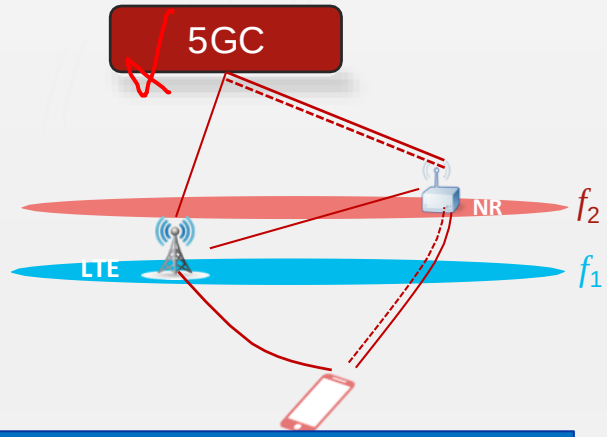
Option 3



Option 7



Option 4

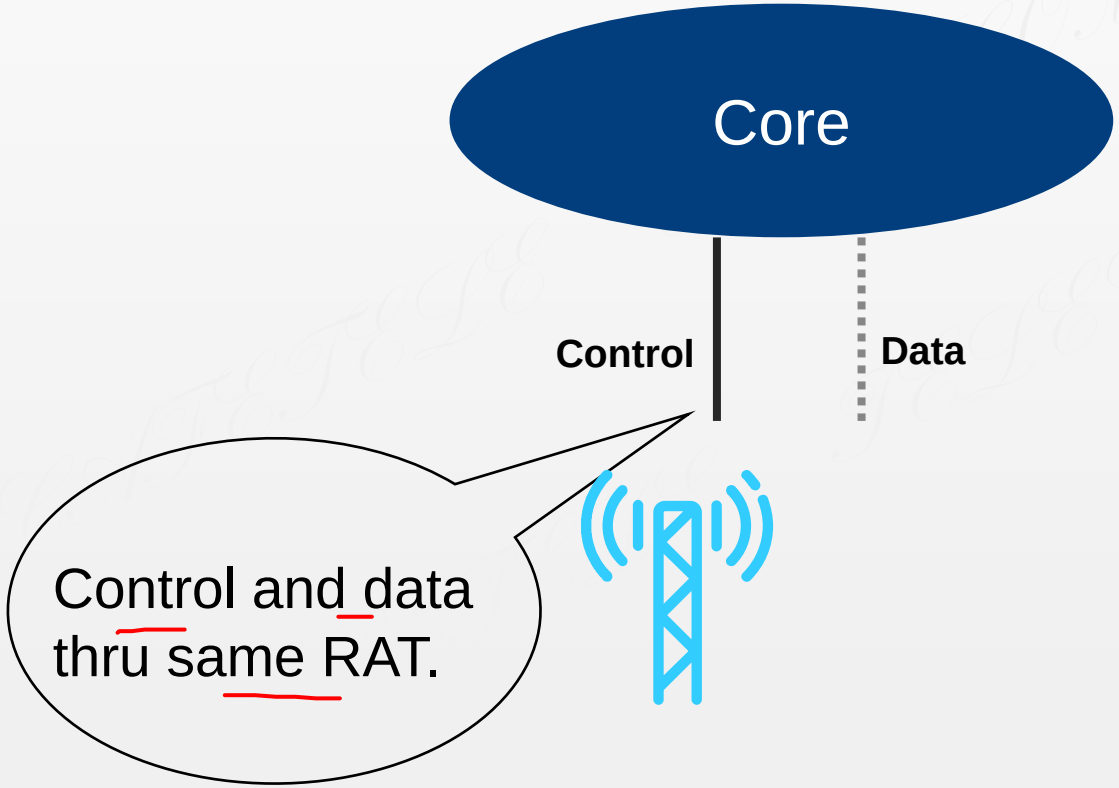


Deployed options depend on Use Cases/Spectrum

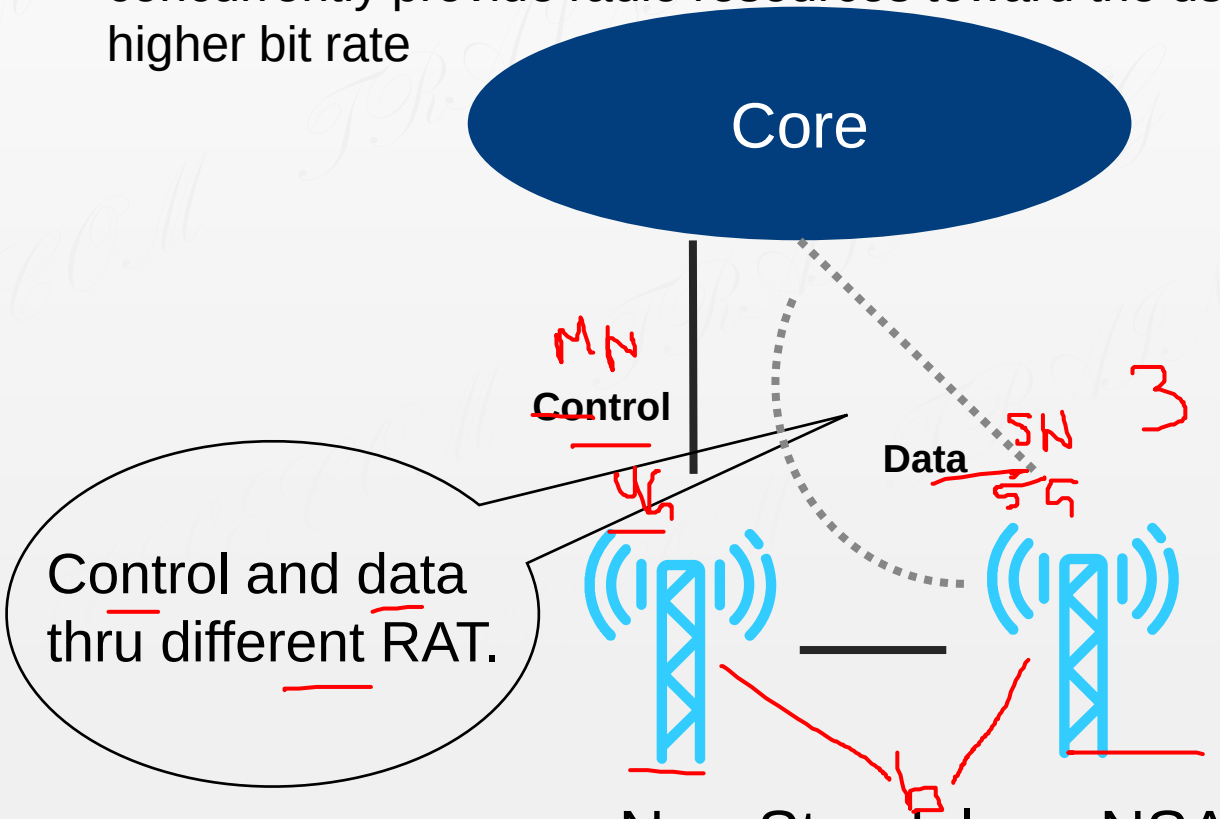
MR DC Architecture

Architecture overview: Standalone vs non-standalone

Dual Connectivity (DC):
A Master Node (MN) and a Secondary Node (SN) concurrently provide radio resources toward the user, for higher bit rate



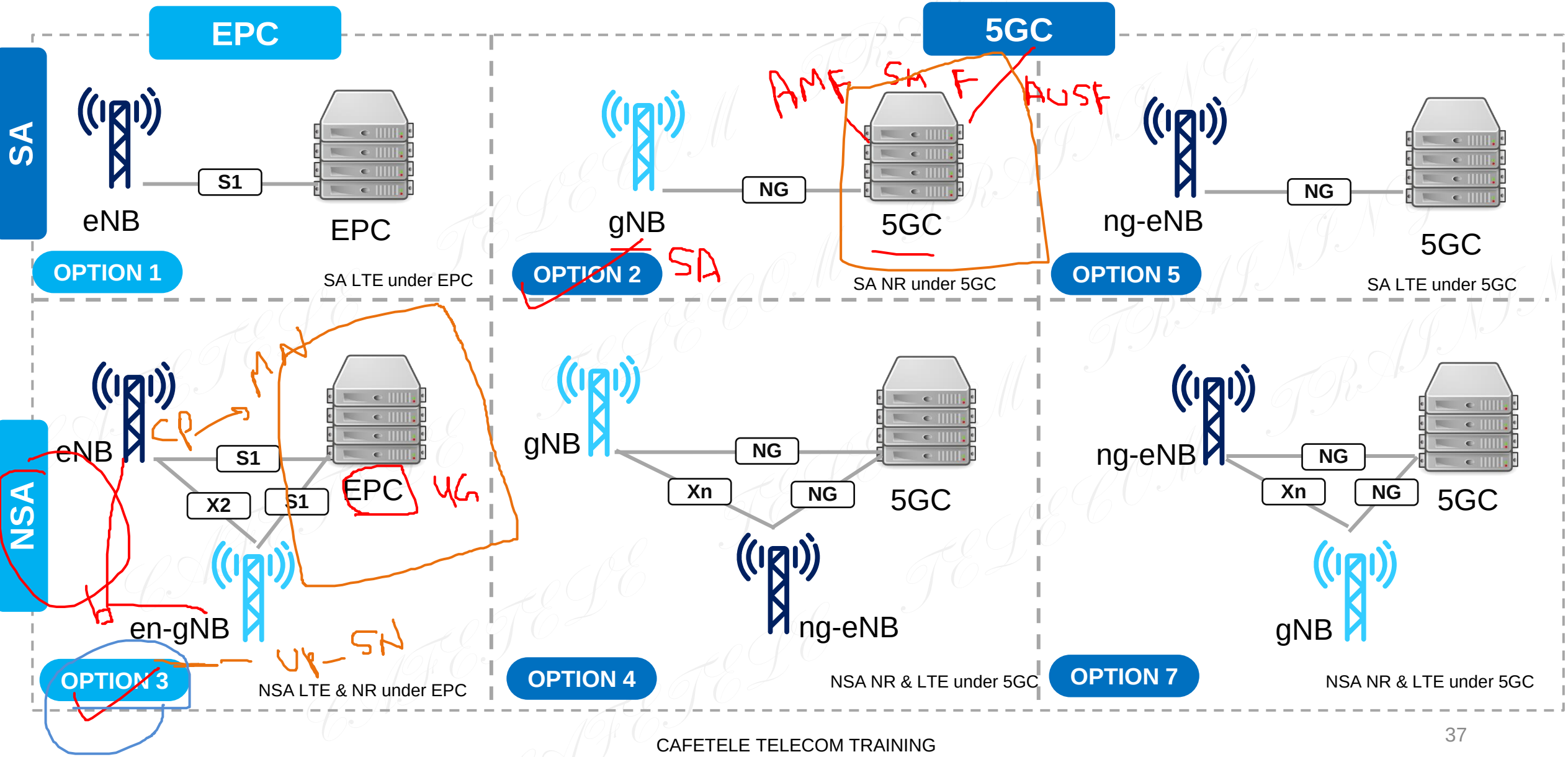
Standalone SA



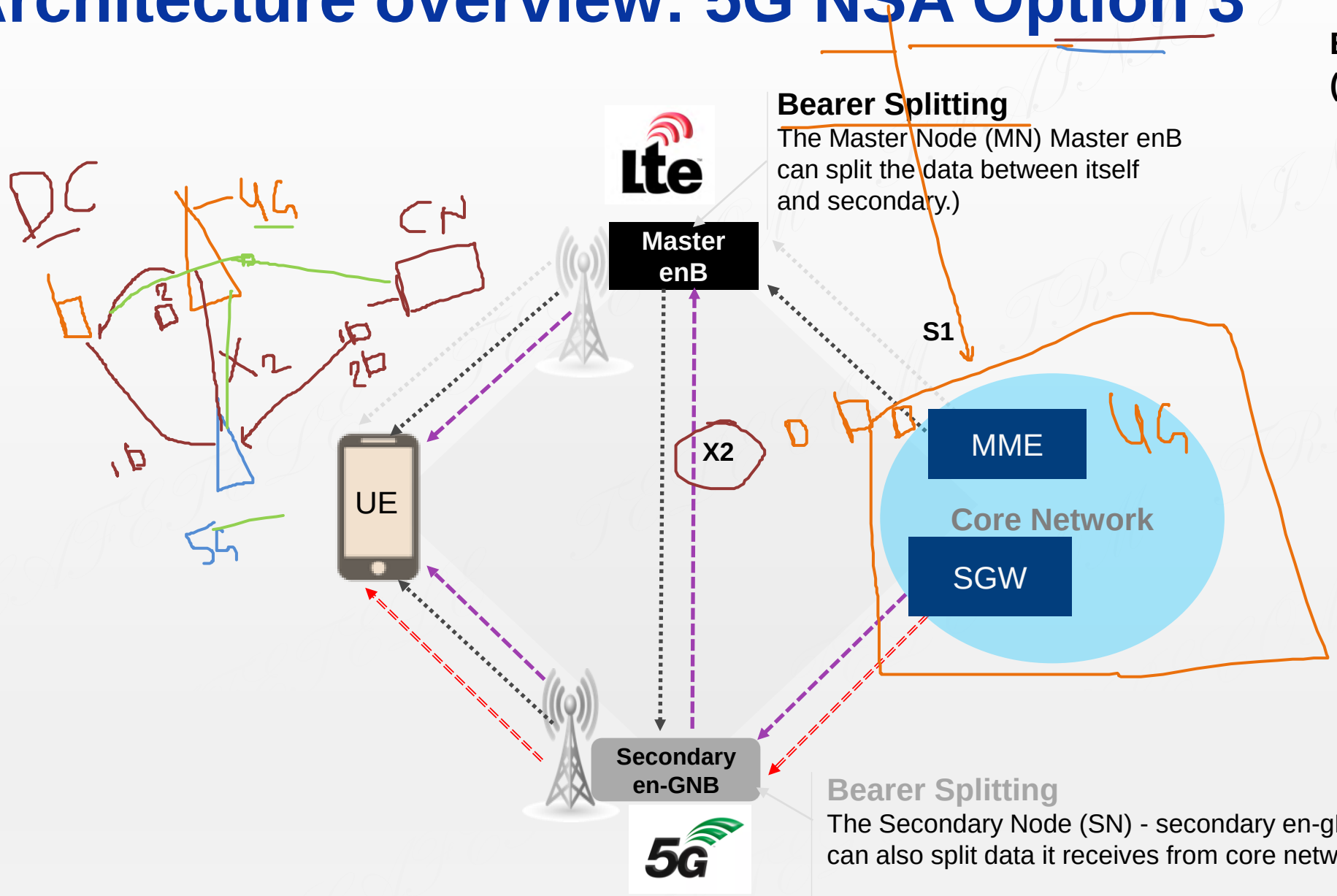
Non-Standalone NSA

The terminal “sees” a Master Cell Group (MCG) and a Secondary Cell Group (SCG)

5G NSA & SA DEPLOYEMENT OPTION



Architecture overview: 5G NSA Option 3



Bearer Splitting
The Master Node (MN) Master enB can split the data between itself and secondary.)

E-UTRA-NR Dual Connectivity (EN-DC)

MCG Bearer

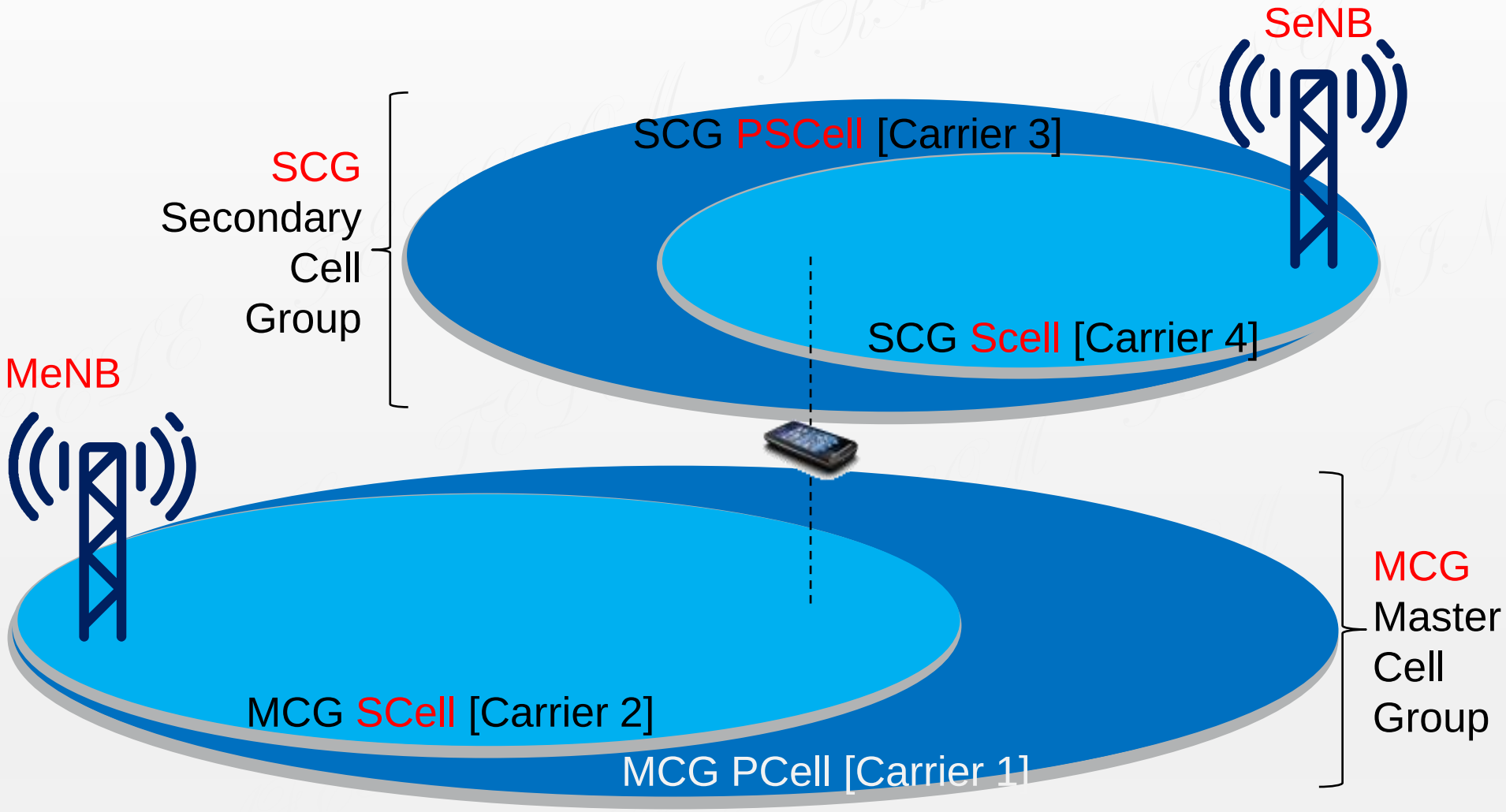
MCG Split Bearer

SCG Bearer

SCG Split Bearer

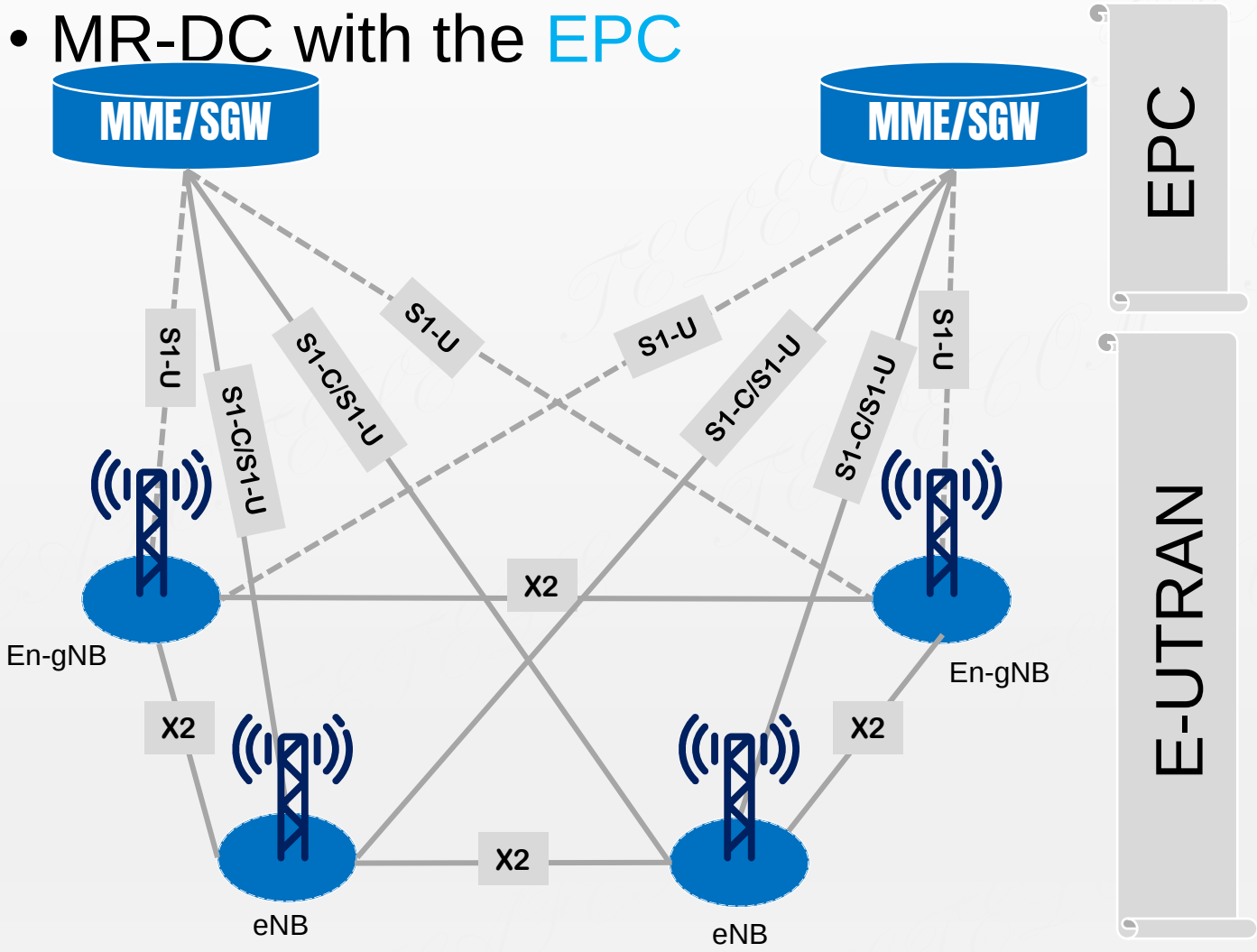
Bearer Splitting
The Secondary Node (SN) - secondary en-gNB can also split data it receives from core network.

What is Dual Connectivity?



Multi-Radio Dual Connectivity(EN-DC)

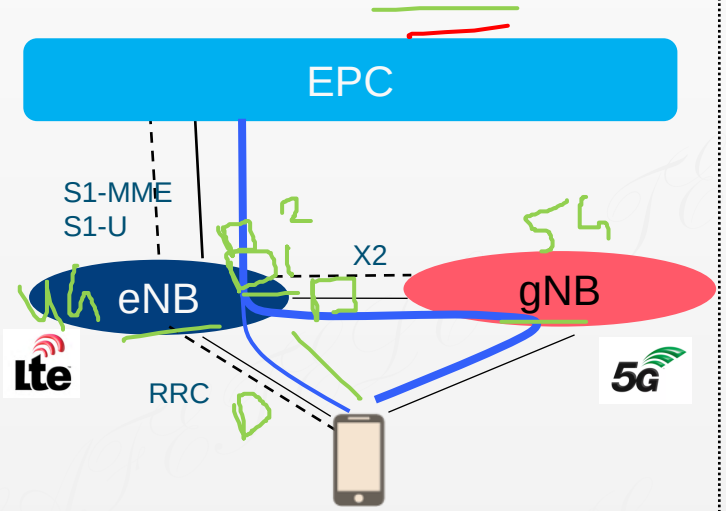
- MR-DC with the EPC



- E-UTRAN supports MR-DC
- eNB acts as a MN
- En-gNB that acts as SN
- eNB connected to EPC via S1
- eNB & en-gNB connected via X2 interface
- En-gNB might also connected to EPC
- via the S1-U interface.
- en-gNB and en-gNB connected via X2 interface

Architecture overview: 5G NSA Option 3 (EN-DC) variants

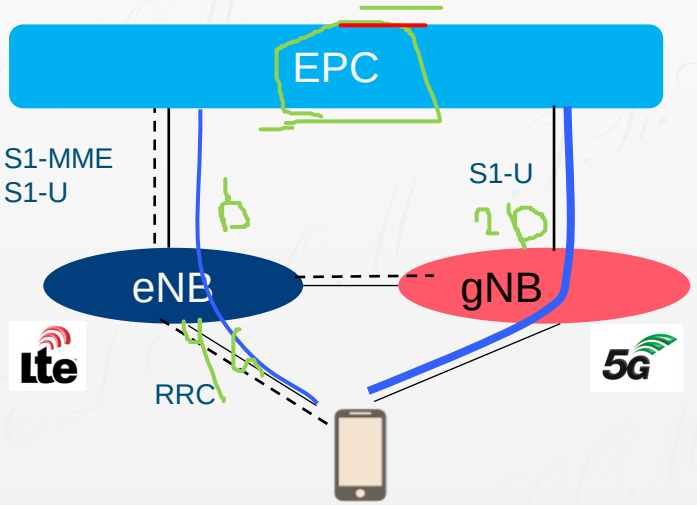
Option 3



- Bearer split in the eNB MCG Split Bearer
- High Load on eNB & LTE BH
- Limited mobility impacts.

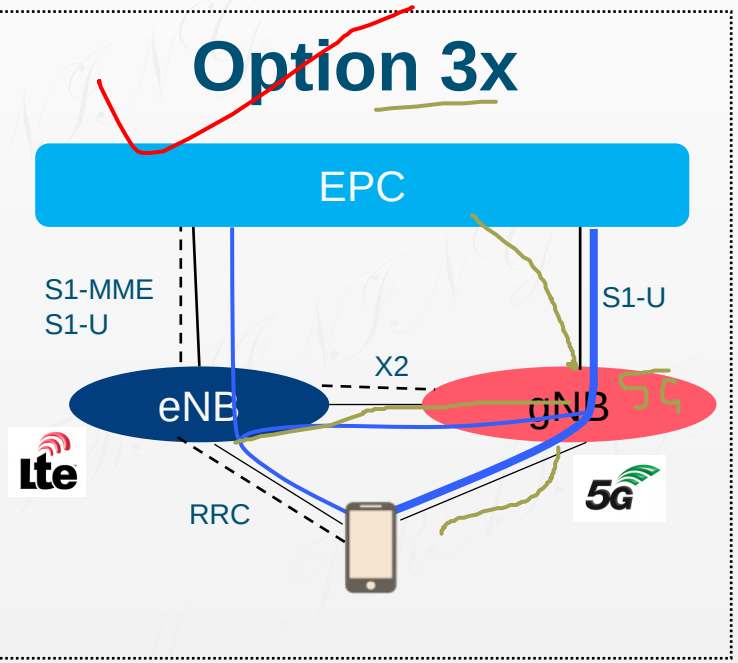
No impact on EPC.

Option 3a



- MCG(Master Cell Group) + SCG(Secondary Cell Group) Bearer.
- Each bearer on LTE or 5G High mobility impacts

Option 3x

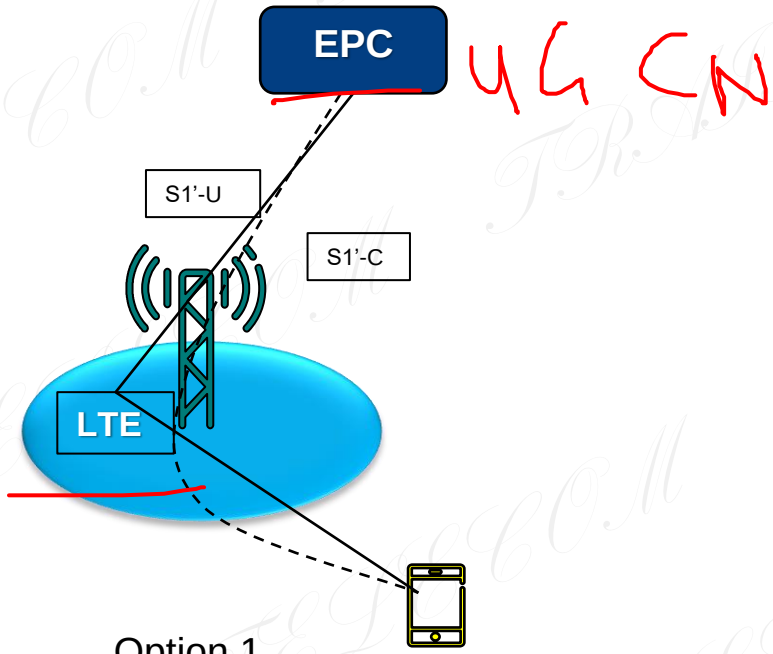


- Bearer split in the gNB SCG Split Bearer
- Limited mobility impacts.

In options 3a/3x the EPC needs to support new E-RAB Modifications procedures to add/remove S1-U bearer to gNB.

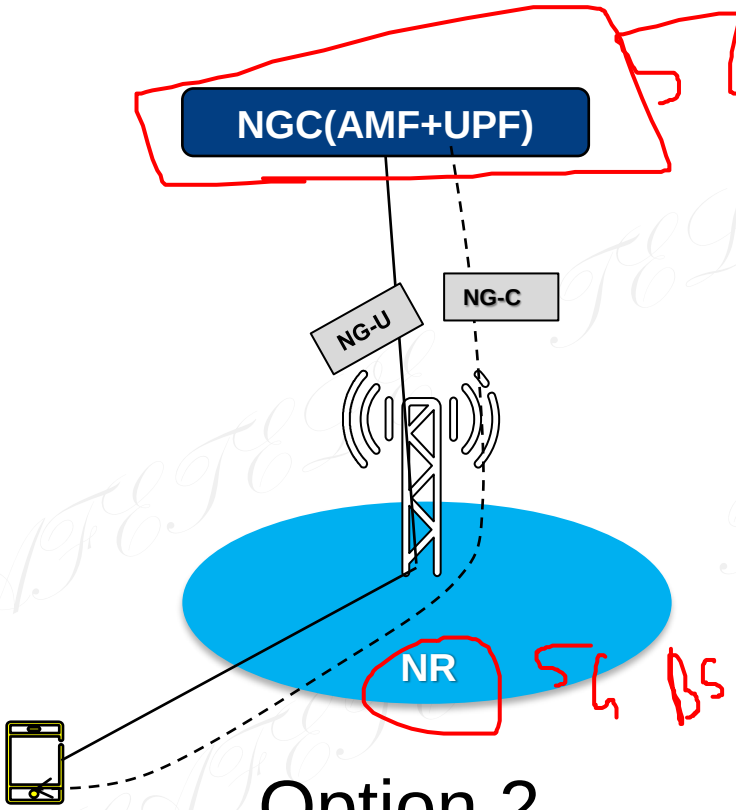
5G SA RAN Architecture

SA LTE connected to EPC - Legacy



Option 1

SA NR connected to 5GC



Option 2

Only option for greenfield 5G operators

- Full support for new 5G applications and services including:

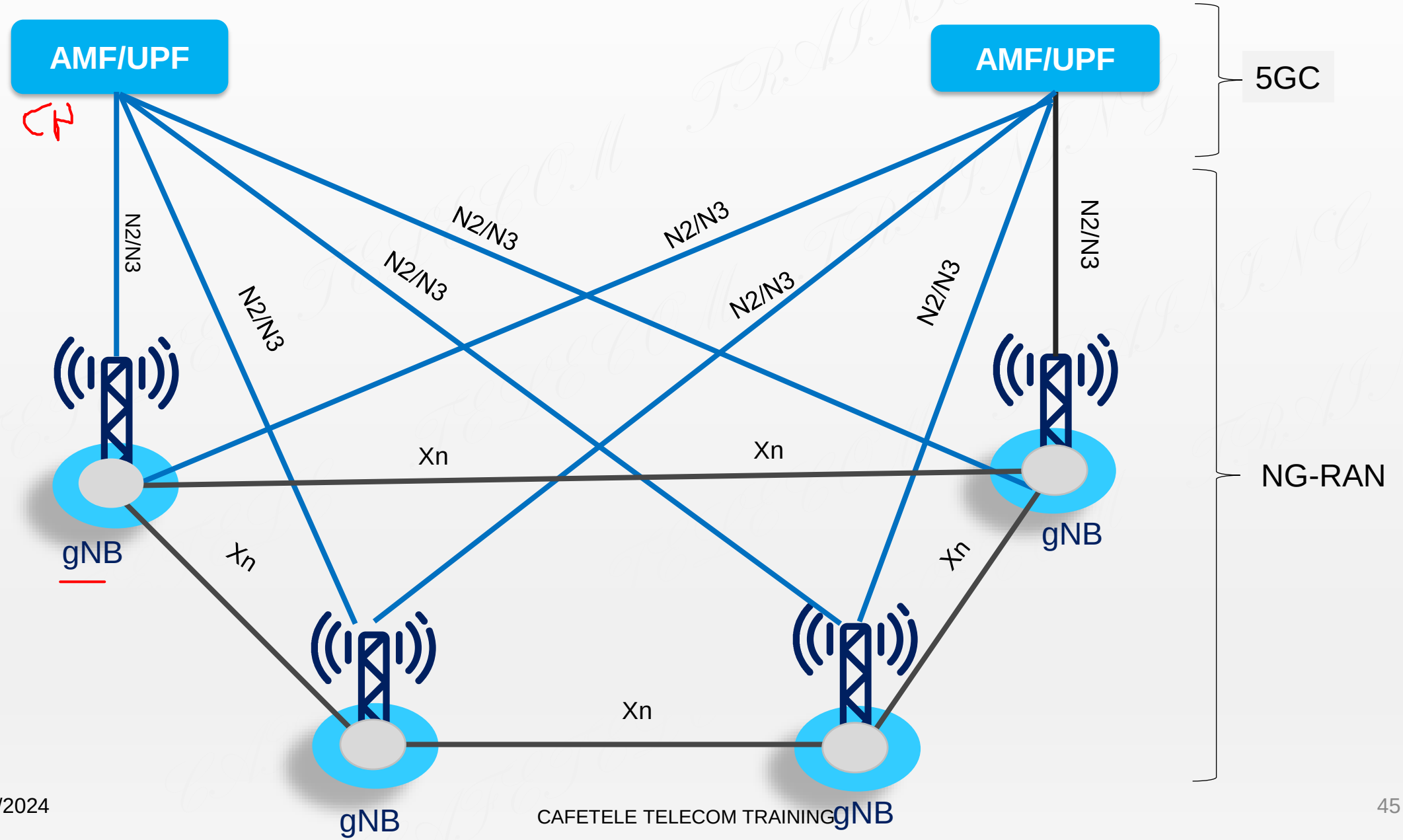
- Enhanced Mobile Broadband (eMBB)

- Massive Machine-Type Communications (mMTC)

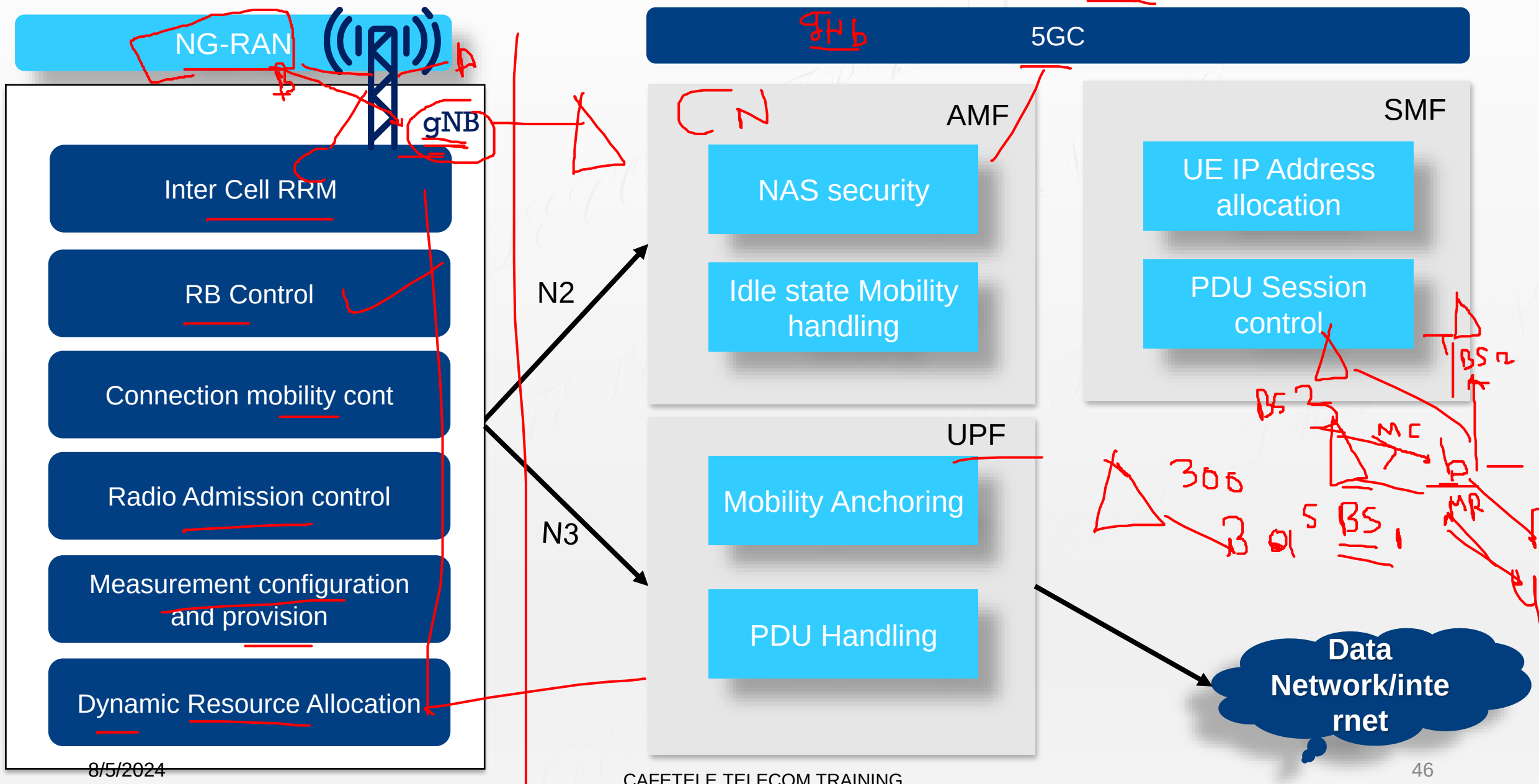
- Ultra-reliable and Low Latency Communications (URLLC)

- Needs multiple spectrum to provide all above cases and also to provide ubiquitous 5G coverage

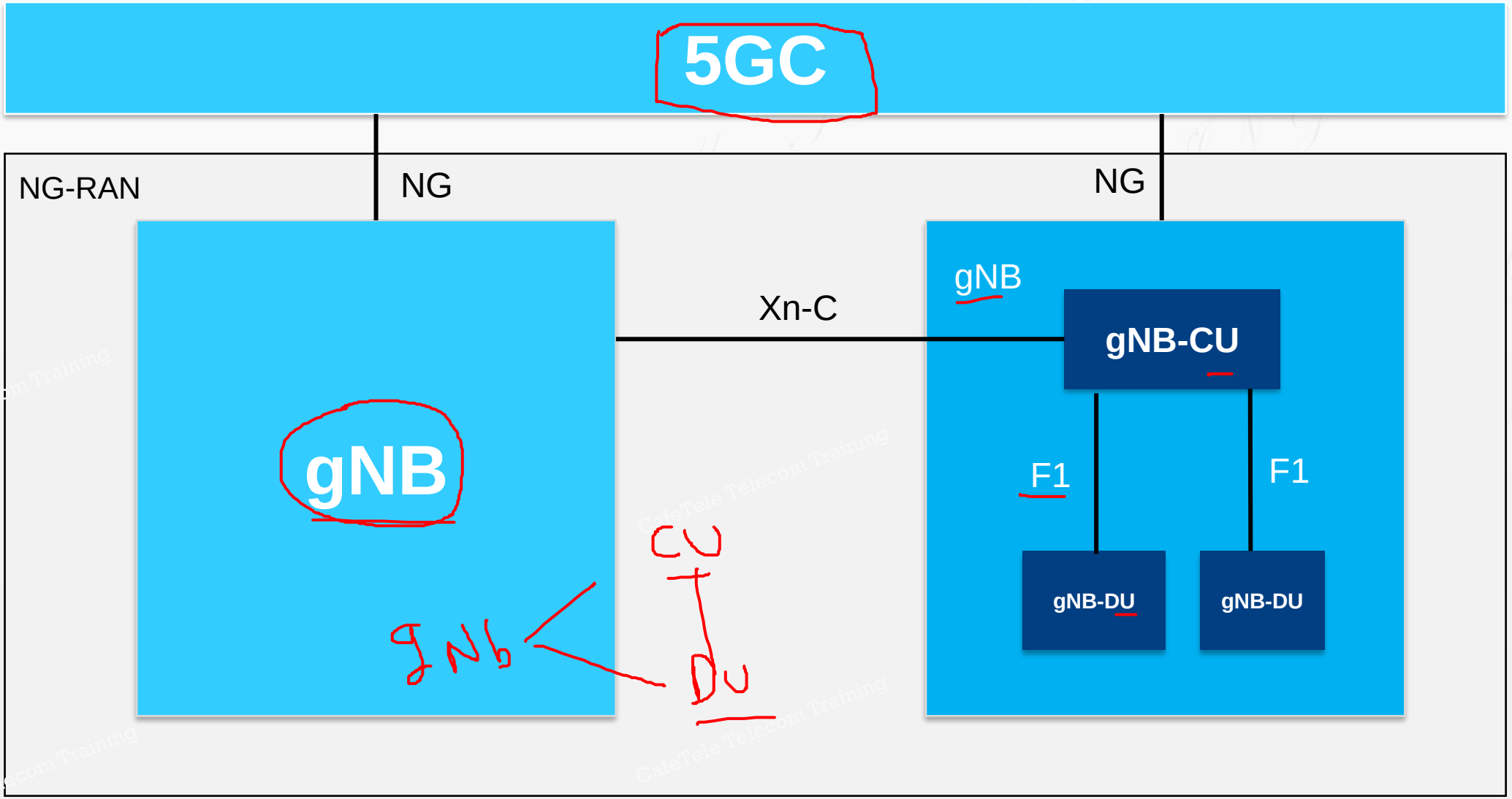
NR Standalone RAN Architecture



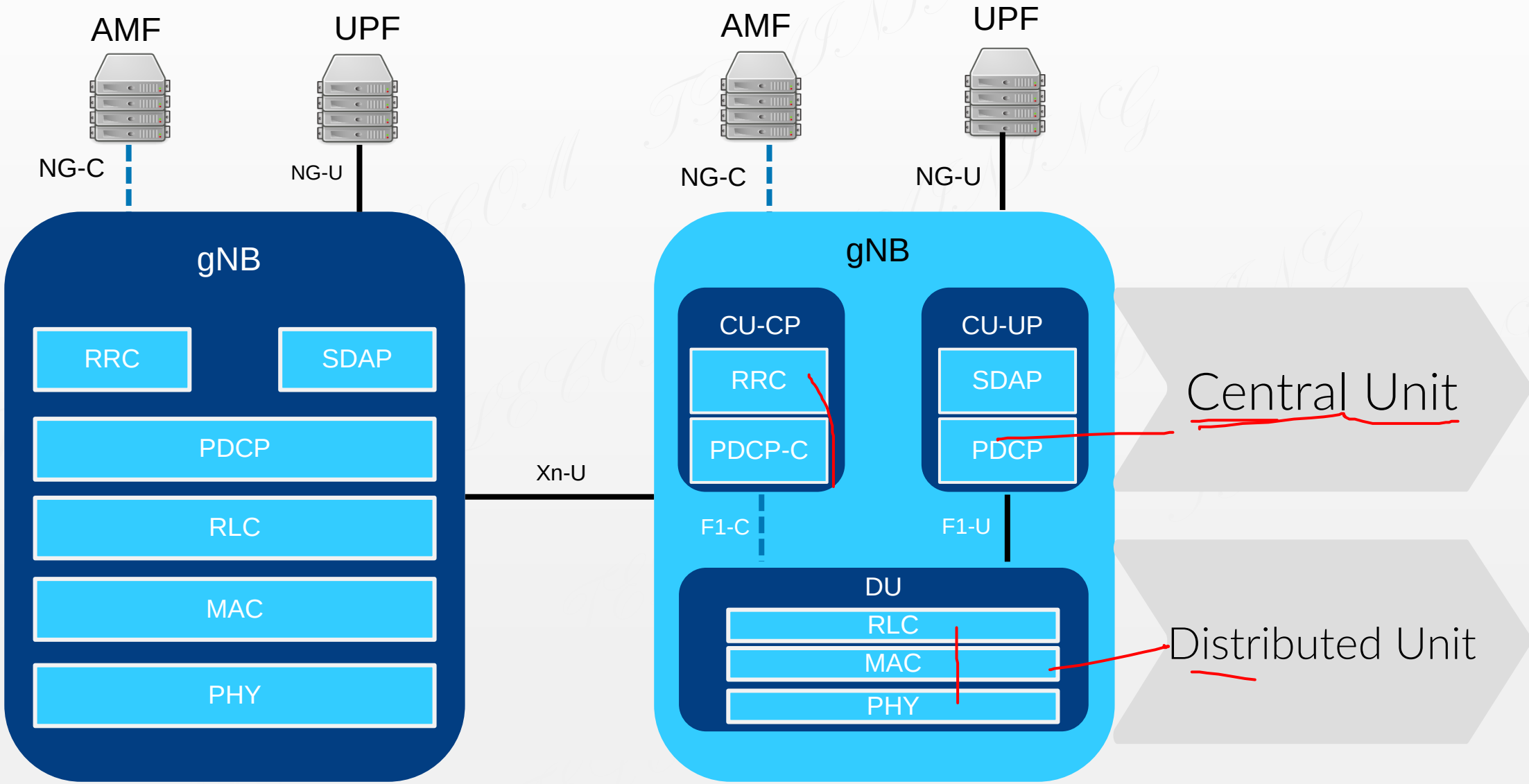
Functional split between NG-RAN and 5GC nodes



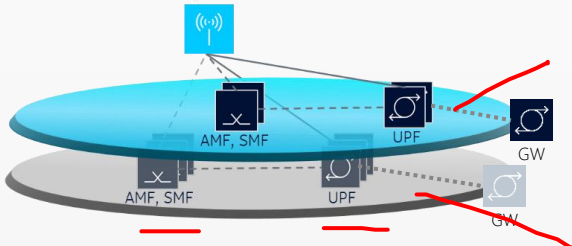
Overall Architecture of NG-RAN



Overall Architecture of NG-RAN

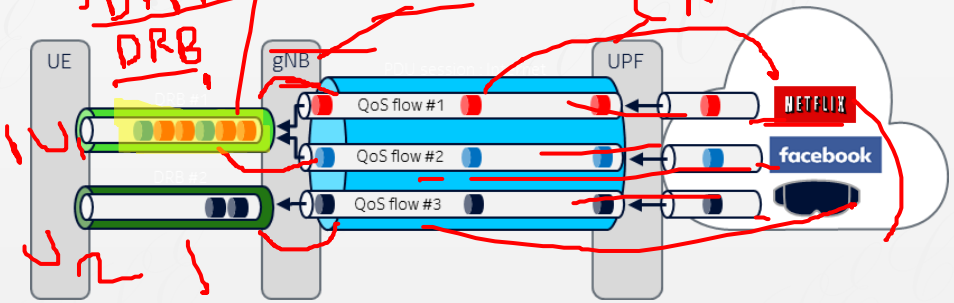


5G Network Slicing



Core

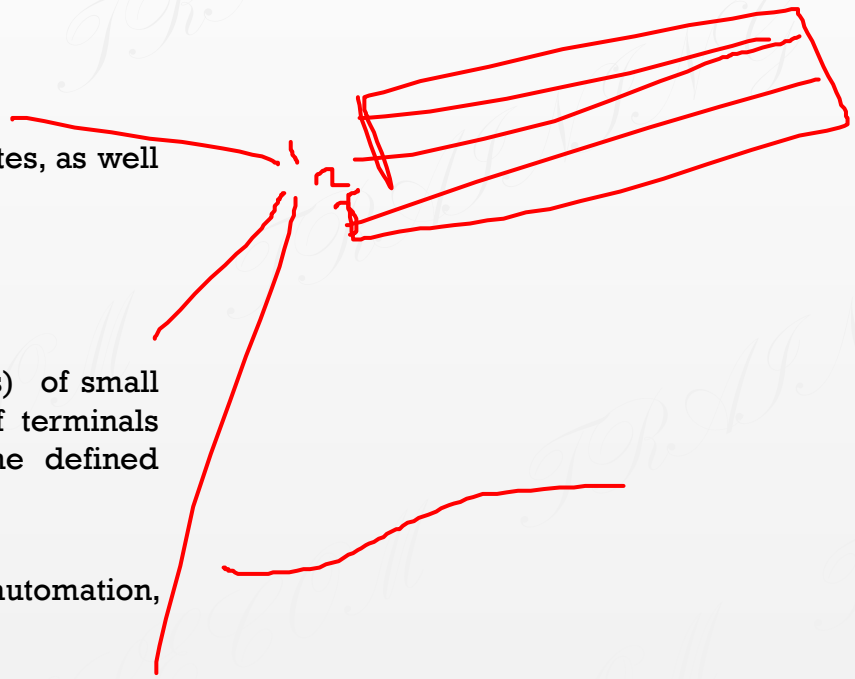
RAN



Transport

Slice Types

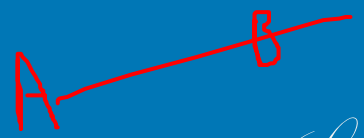
- Currently there are three standardized slices:
  - **eMBB (5G enhanced mobile broadband): SST = 1**
    - it supports stable connections with very high peak data rates, as well as moderate rates for cell-edge users,
    - higher user mobility, high capacity,
    - latency of around 1ms for user experienced data exchange.
  - **URLLC (ultra reliable low latency communication): SST = 2**
    - It supports low-latency transmissions (much less than 1ms) of small payloads with very high reliability from a limited set of terminals (comparing to MIoT), which are active according to the defined patterns,
    - This is machine type, mission-critical communication type,
    - Use cases: remote surgery, autonomous vehicles, factory automation, electrical power distribution.
  - **MIoT (slice for handling massive IoT): SST = 3**
    - supports massive number of small IoT devices which are only sporadically active and send small data payloads,
    - it needs to support a very large number of devices in a small area,
    - in this feature latency is less than 1 ms and targeted reliability is 99.99%
- Next standardized slices are under definition in 3GPP



5G NR Protocols

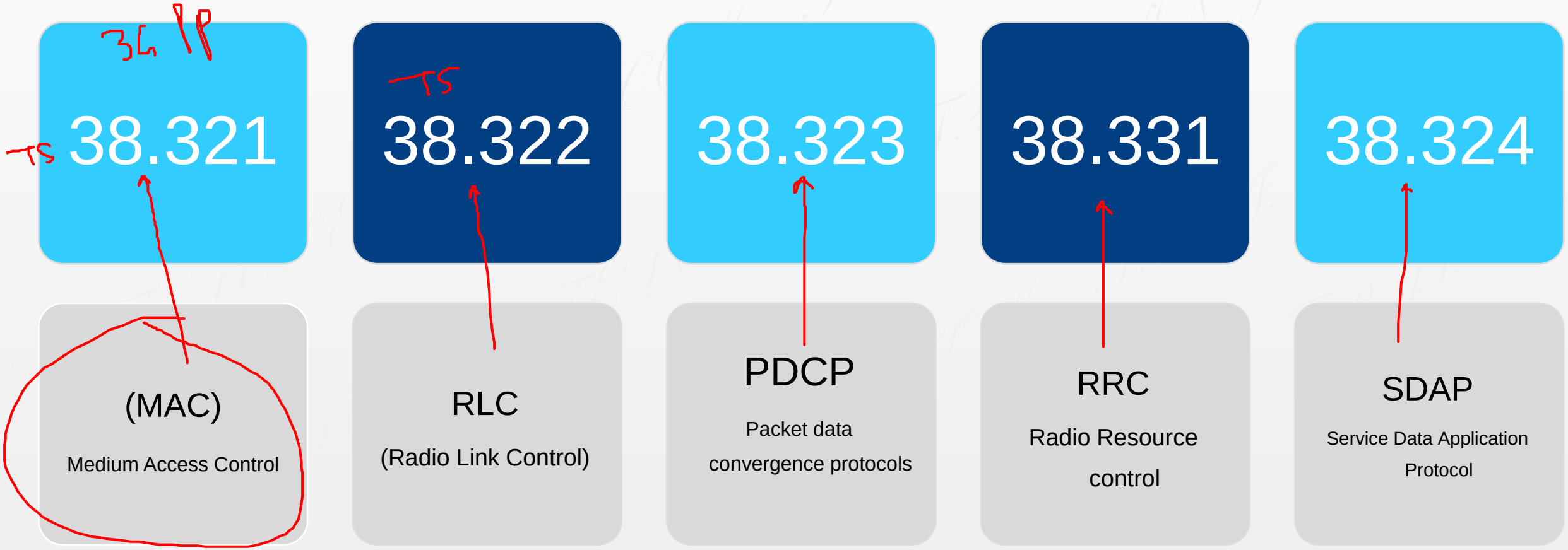
Module 3

- Control Plane Protocol L2
- User Plane Protocol L2
- SDAP Protocol
- PDCP Protocol
- RLC Protocol (TM,AM,UM)
- MAC Protocol



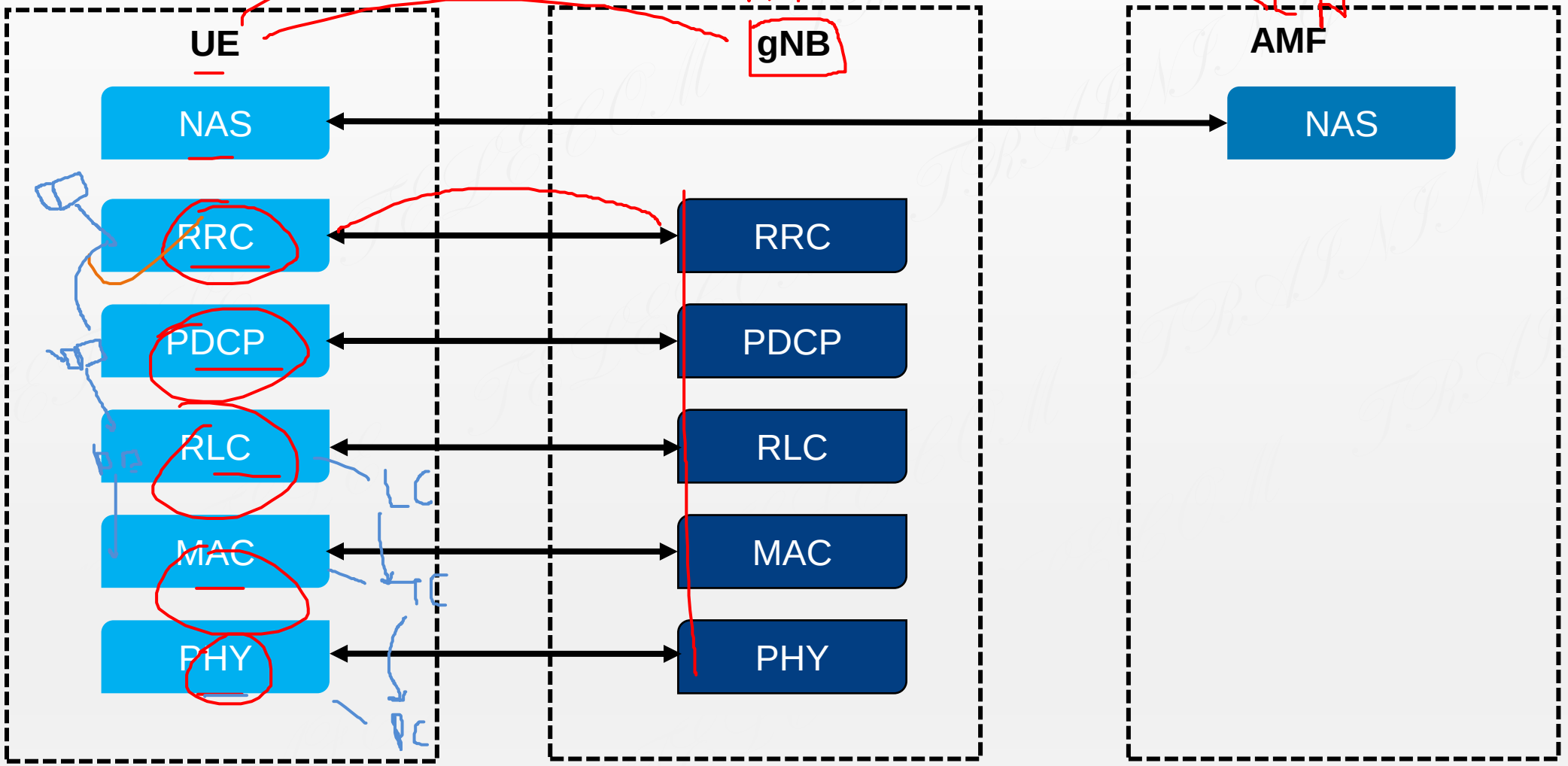
5G NR PROTOCOLS

5G NR Protocols

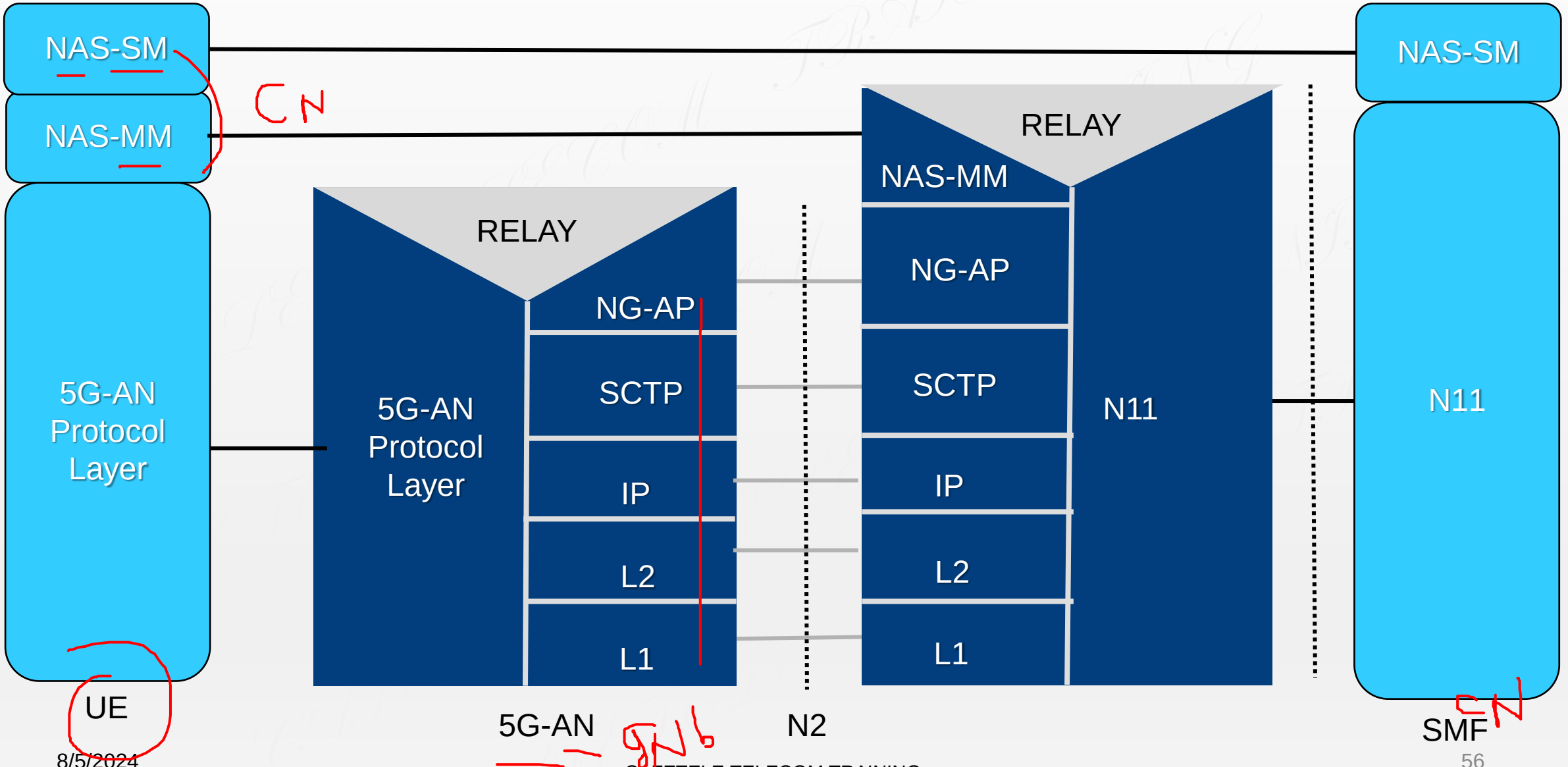


Control Plane Protocols

Control plane protocol stack for NR

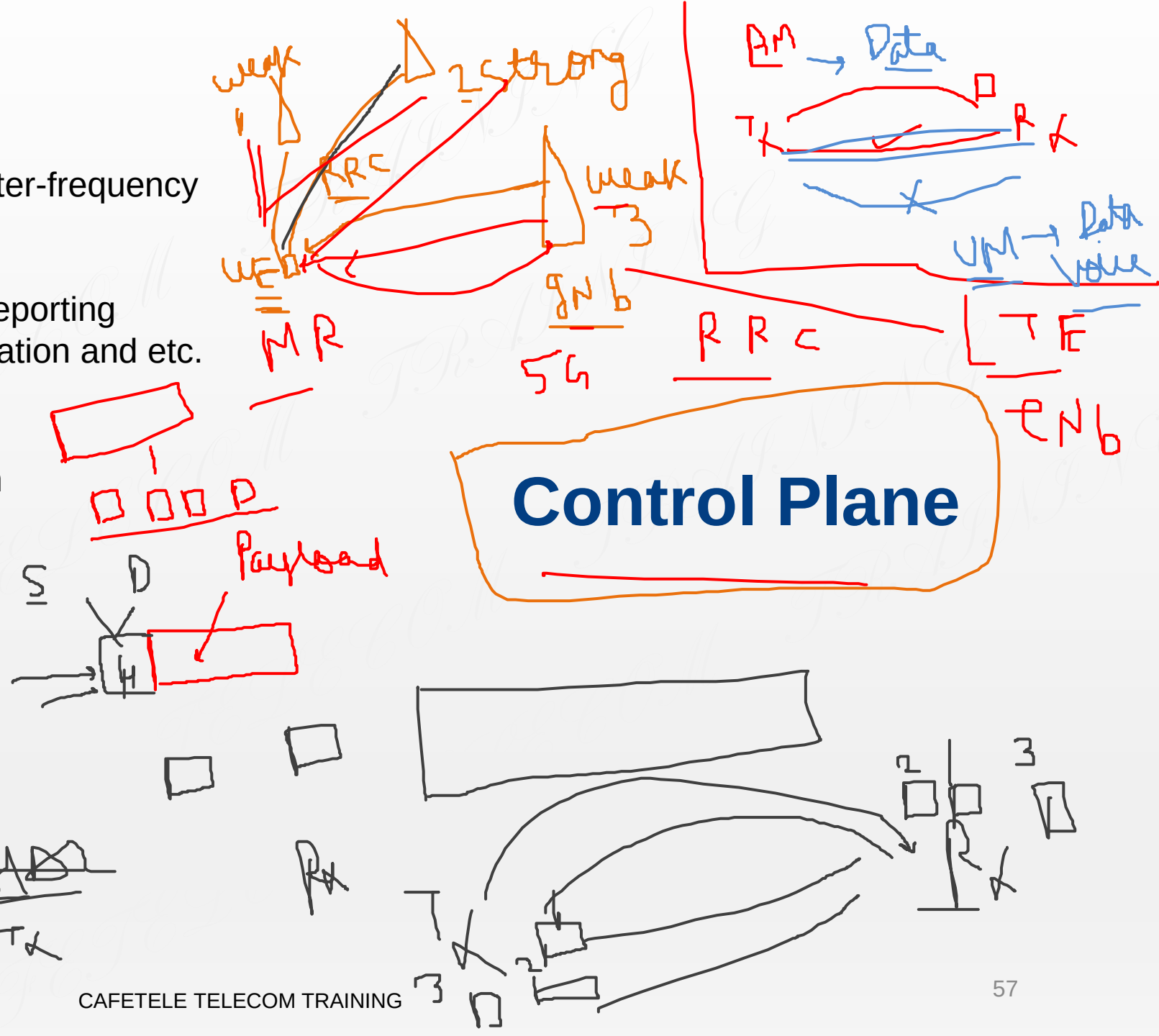


Control Plane Protocol Stack between UE and 5GC



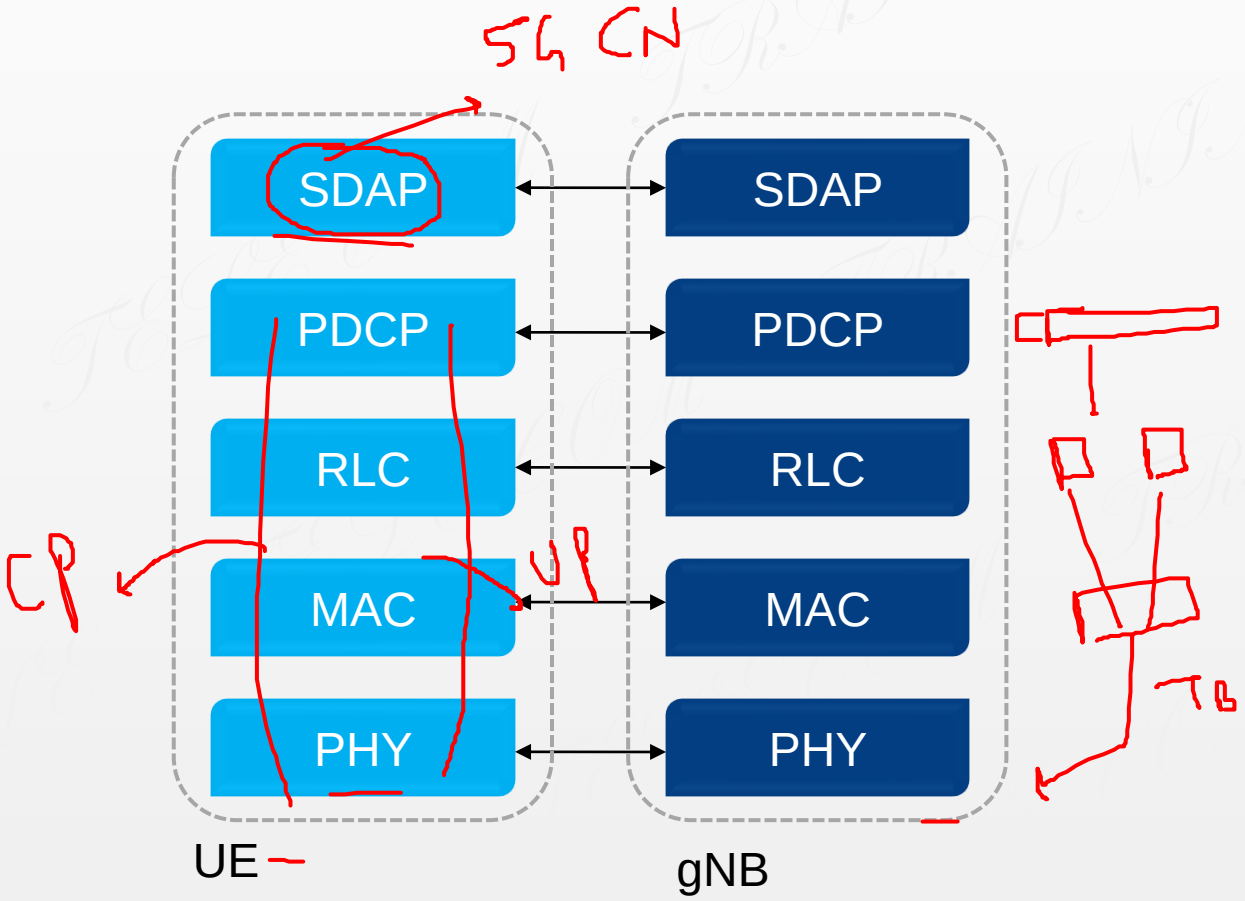
Control Plane

- **RRC**
  - Broadcast of system information
  - RRC connection control & intra/inter-frequency mobility
  - Inter-RAT mobility
  - Measurement configuration and reporting
  - Transfer of dedicated NAS information and etc.
- **PDCP**
  - Header compression, reordering
  - split bearer / duplication operation
  - Ciphering, integrity protection
- **RLC**
  - TM, UM, AM
  - Out of sequence delivery
- **MAC**
  - Multiplexing / Demultiplexing
  - Scheduling information reporting
  - RA Control
  - DRX Control …

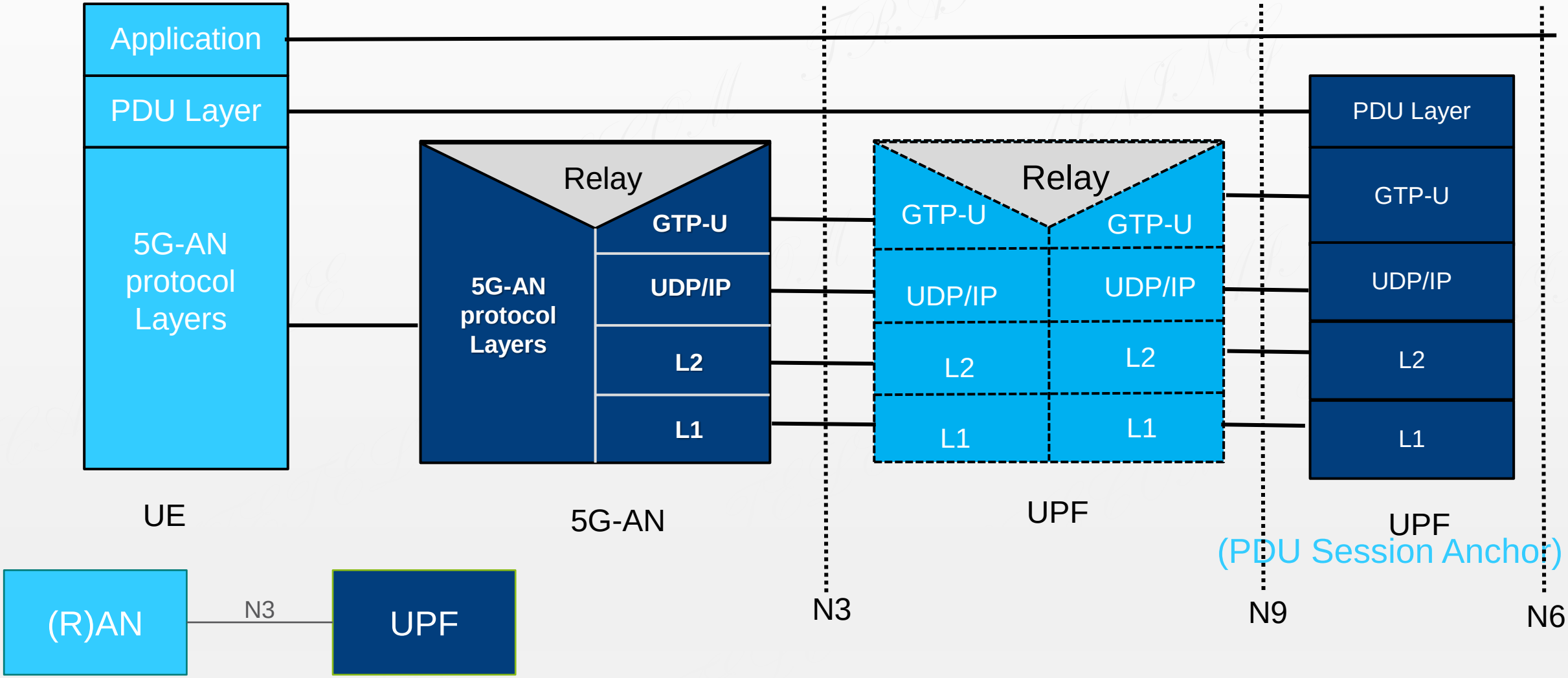


User Plane Protocol Stack

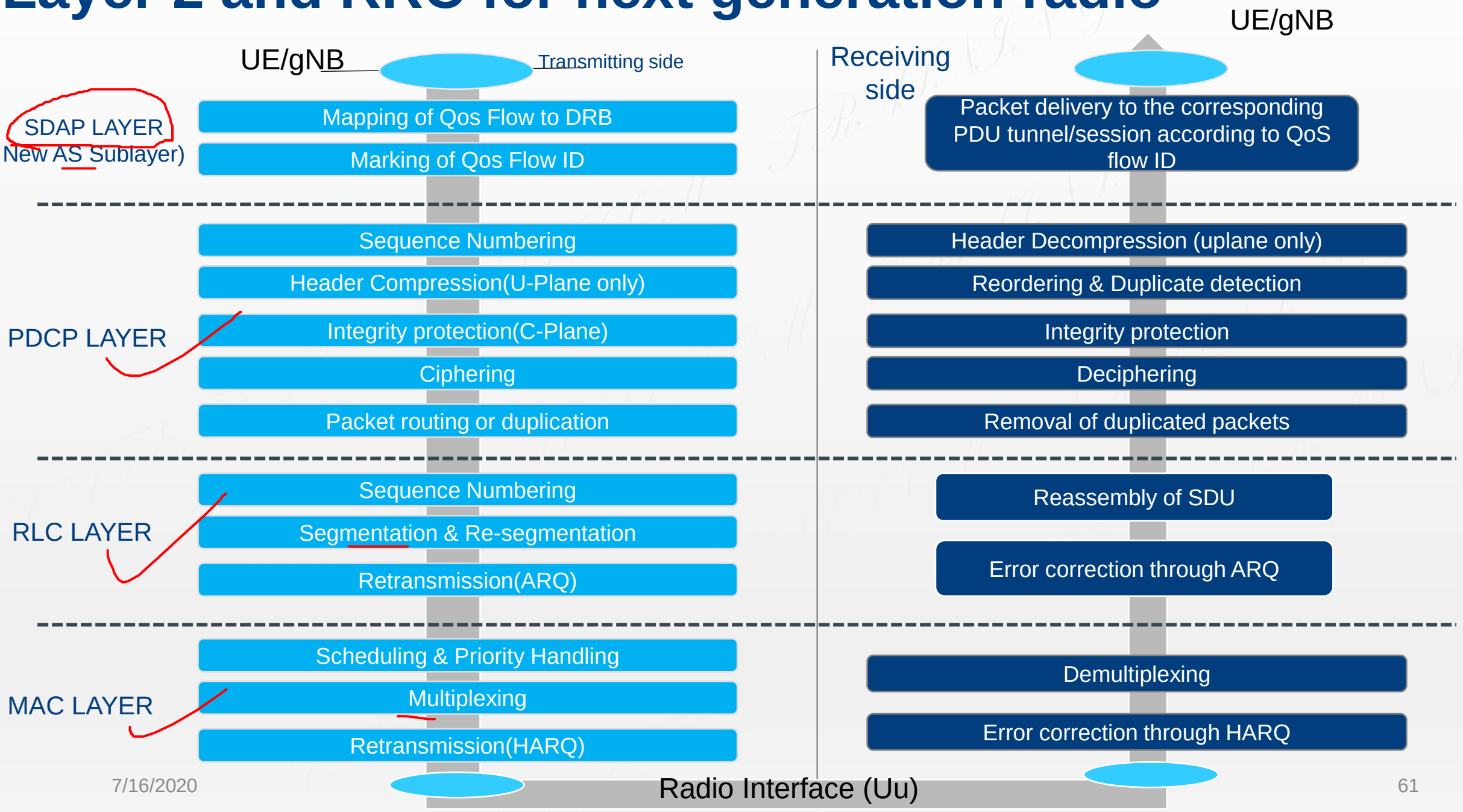
User Plane PROTOCOL



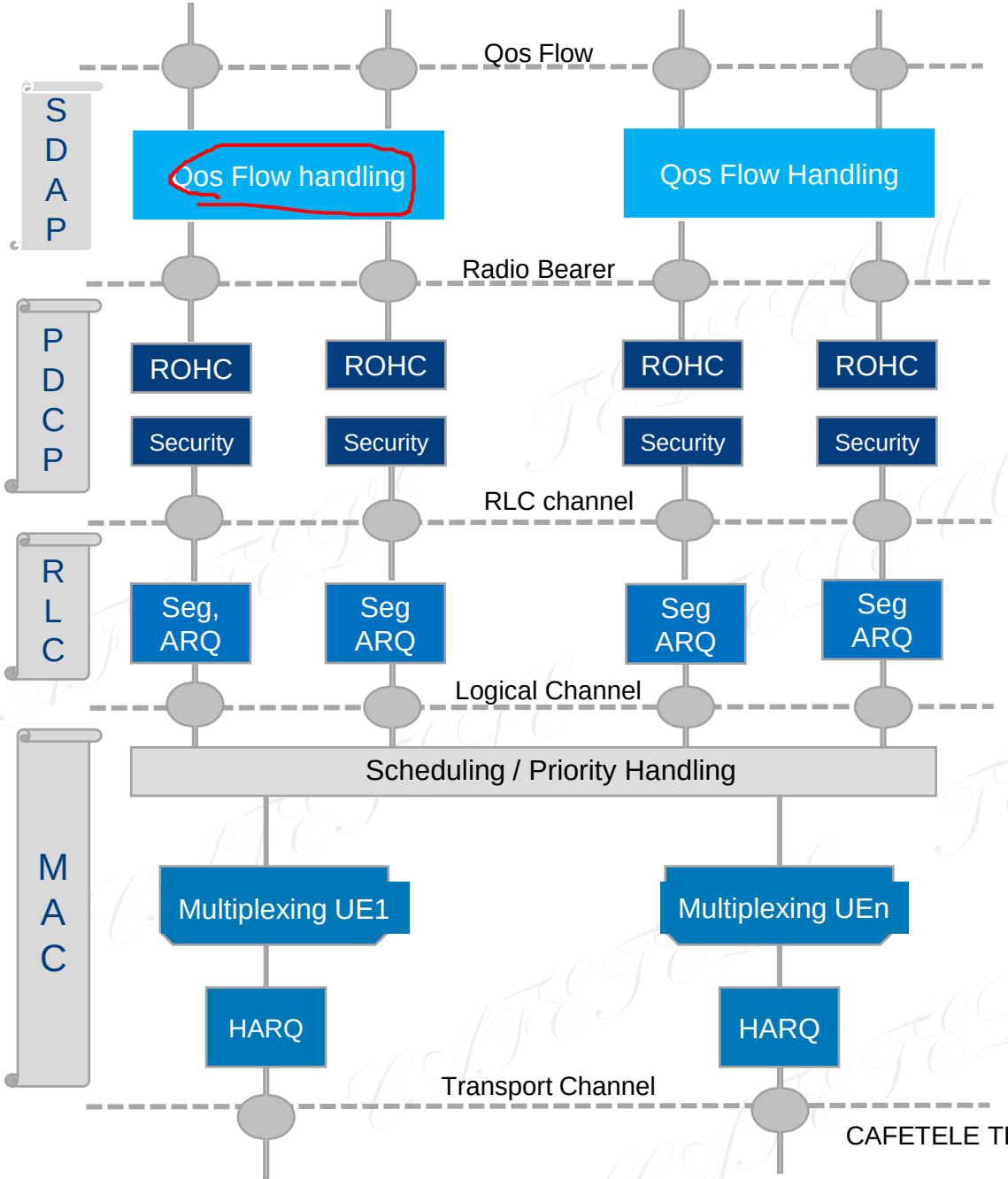
User Plane Protocol Stack for a PDU Session



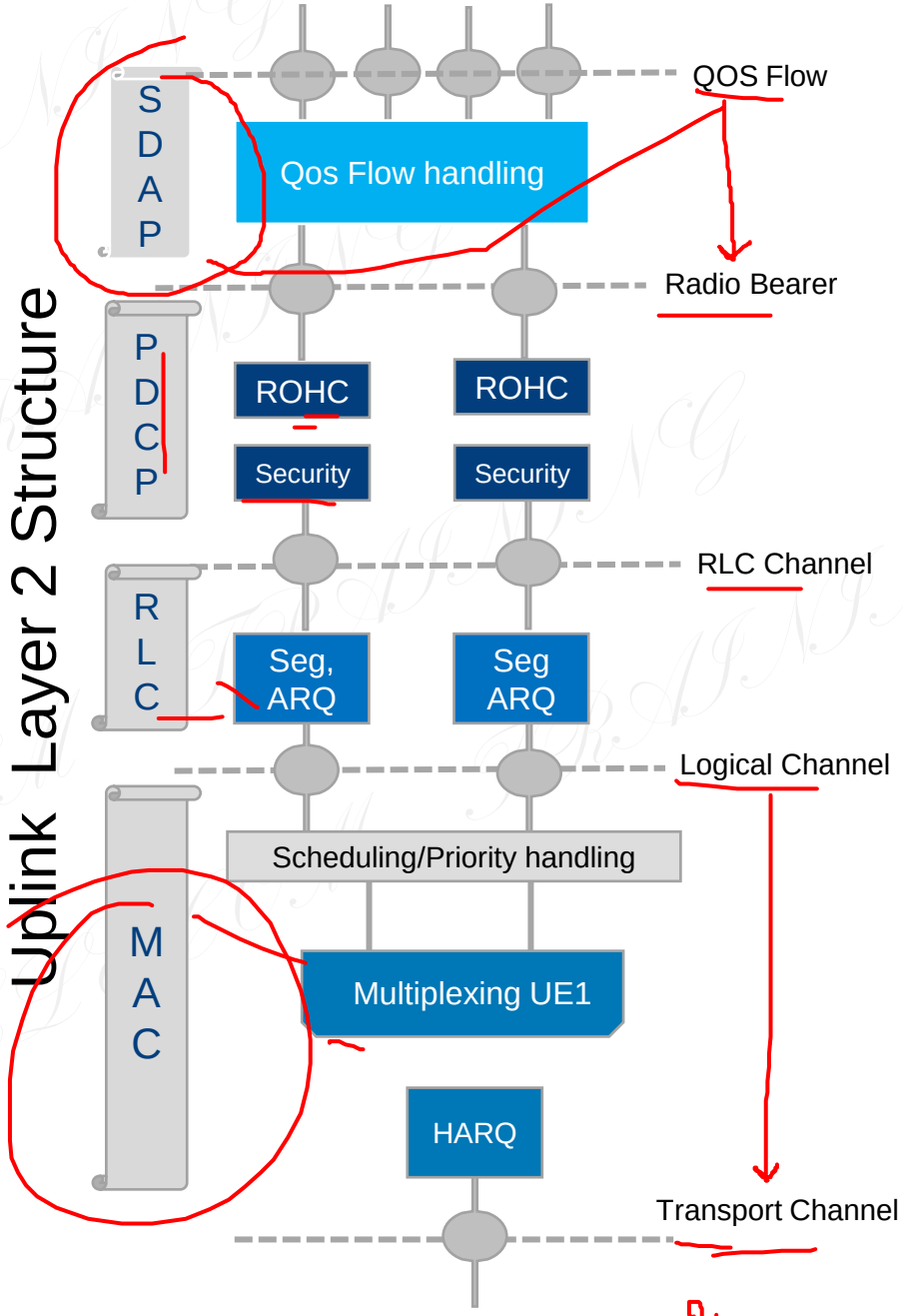
Layer 2 and RRC for next generation radio



Data flow example through Layer 2 protocol stack in NR system

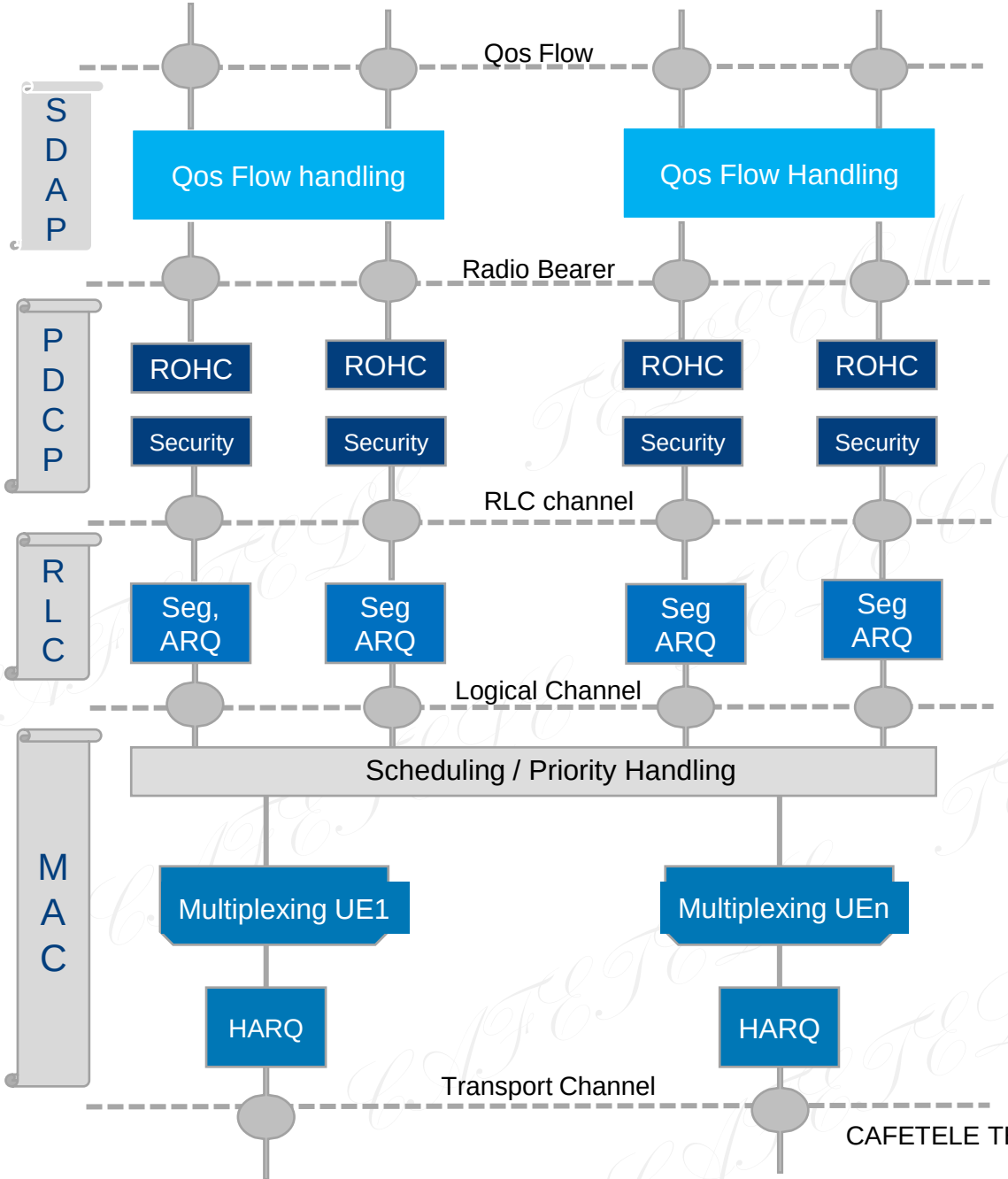


Downlink Layer 2 Structure



Uplink Layer 2 Structure

Data flow example through Layer 2 protocol stack in NR system



Downlink Layer 2 Structure

SADP

- Mapping between QoS flow and DRB
- QoS flow ID (QFI) marking

PDCP

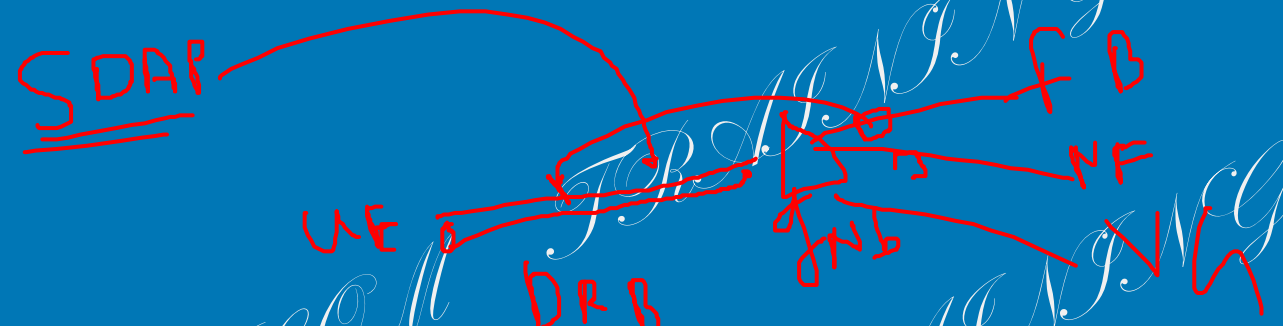
- Header compression, reordering,
- split bearer / duplication operation
- Ciphering, Integrity protection

RLC

- TM, UM, AM
- Segmentation
- ARQ

MAC

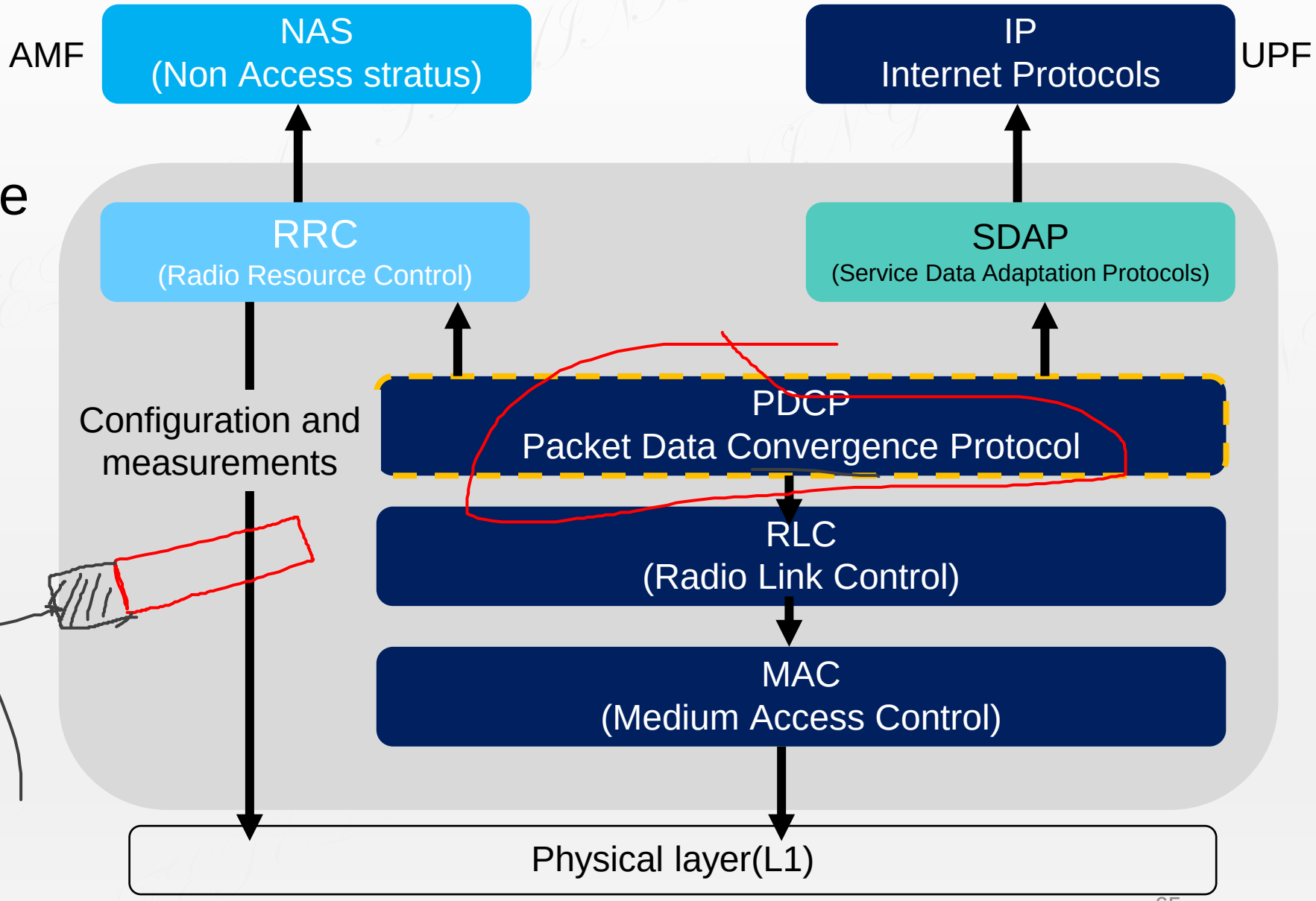
- Multiplexing / Demultiplexing
- Scheduling information reporting
- DRX Control
- Activation / Deactivation
- Beam Failure Recovery ...



Packet Data Convergence Protocol (PDCP)

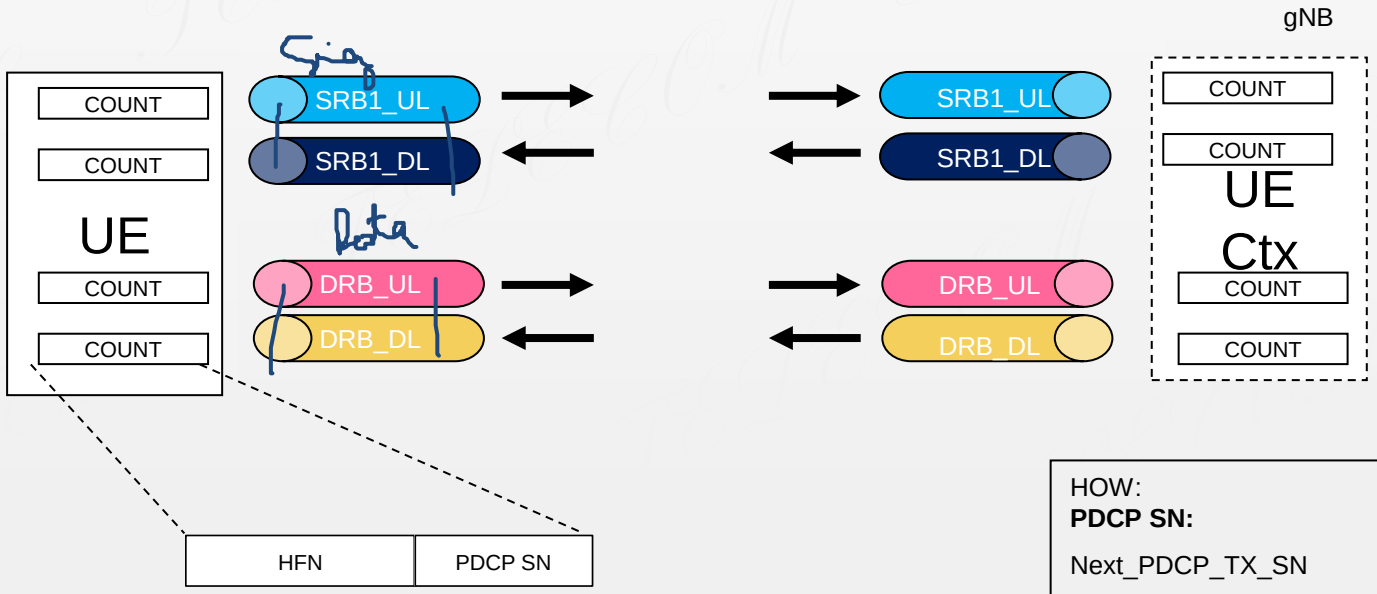
Packet Data Convergence Protocol

- Transfer of user plane data
- Transfer of control plane data
- IP Header compression
- Integrity protection(CP)
- Ciphering(UP & CP)



Sequence Numbering

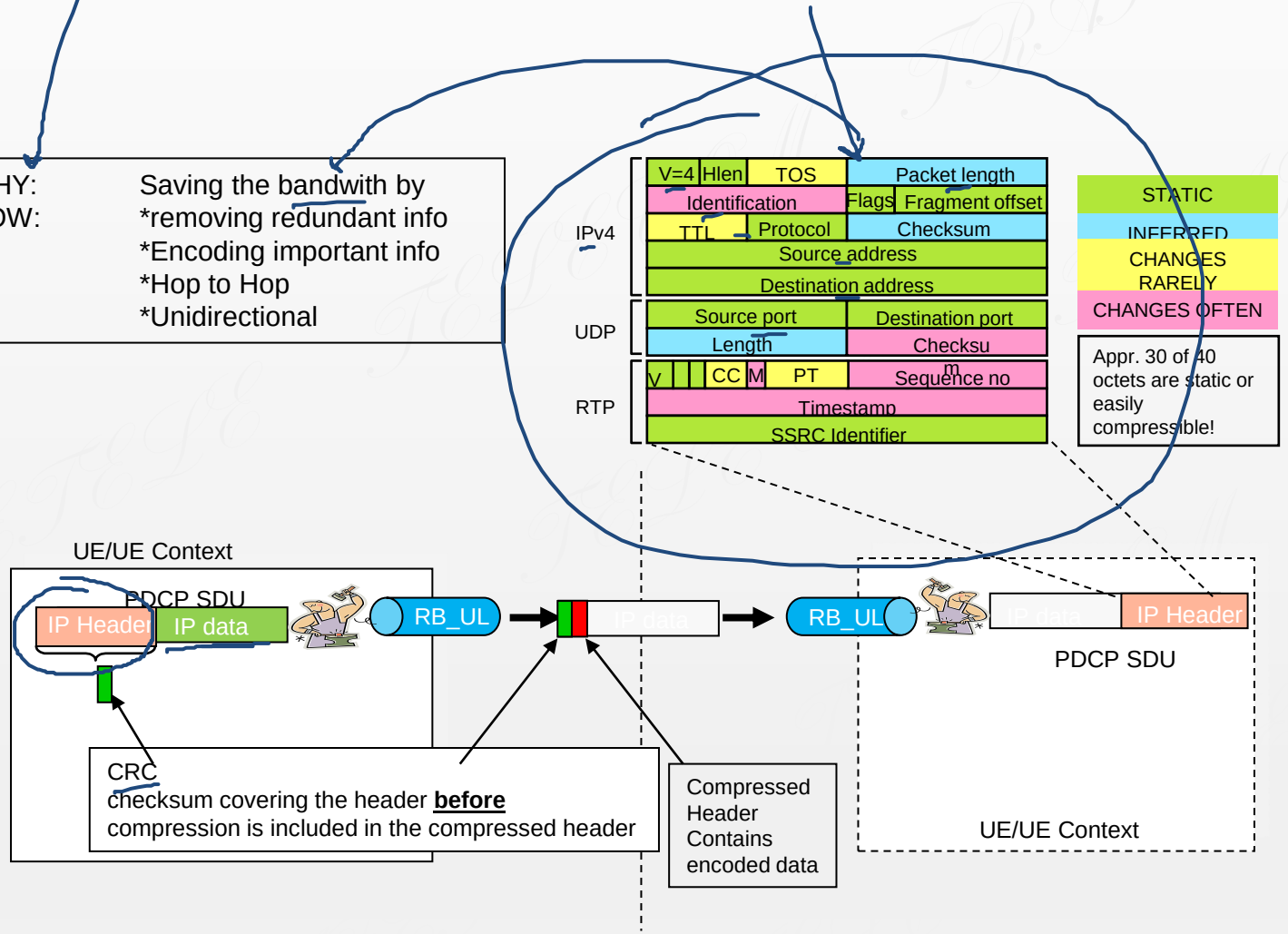
WHY:
* Reordering
* Duplicate detection
* Integrity protection
* Ciphering



HOW:
PDCP SN:
Next_PDCP_TX_SN
TX_HFN
COUNT

Header Compression

WHY: Saving the bandwith by
HOW: *removing redundant info
*Encoding important info
*Hop to Hop
*Unidirectional



Supported profiles	
Profile Identifier	**Usage**
0x0000	No compression
0x0001	RTP/UDP/IP
0x0002	UDP/IP
0x0003	ESP/IP
0x0004	IP
0x0006	TCP/IP
0x0101	RTP/UDP/IP
0x0102	UDP/IP
0x0103	ESP/IP
0x0104	IP

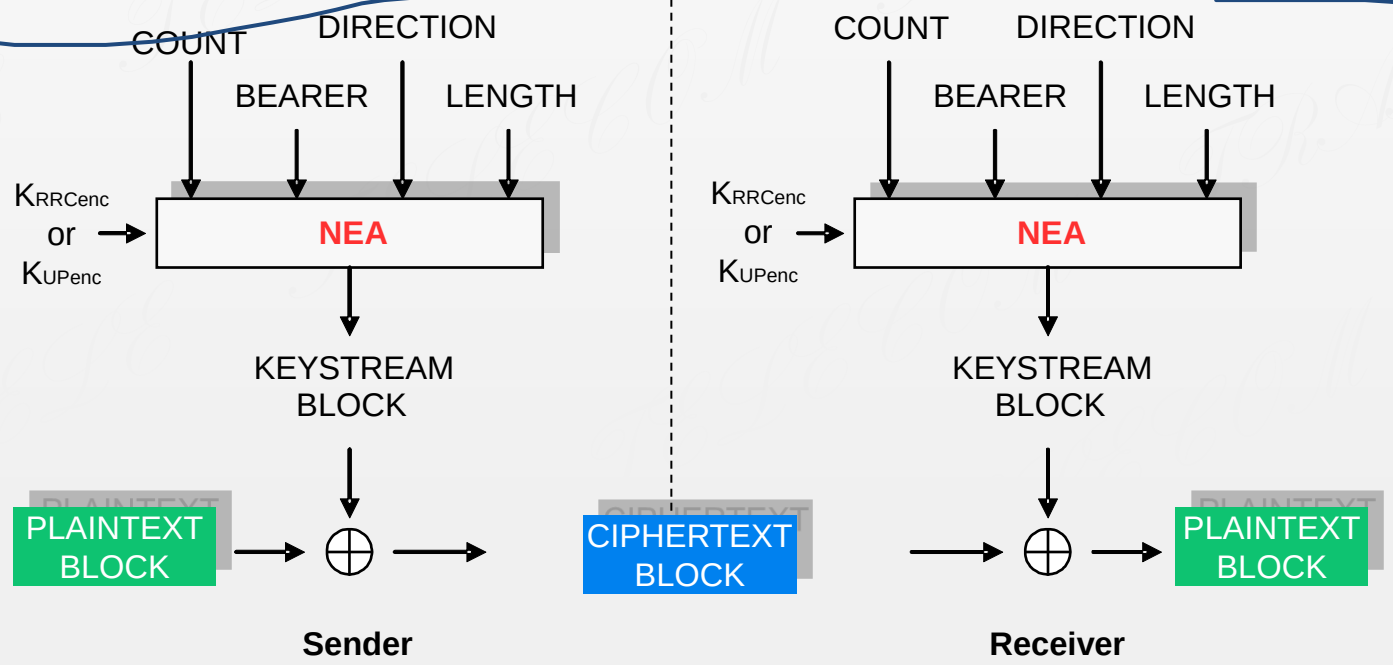
ROHC is only applied to IP packets
Not to SDAP header

Thus, PDCP layer needs to know:
If SDAP layer adds the SDAP header
Length of SDAP header

Ciphering

WHY: To protect the data over radio

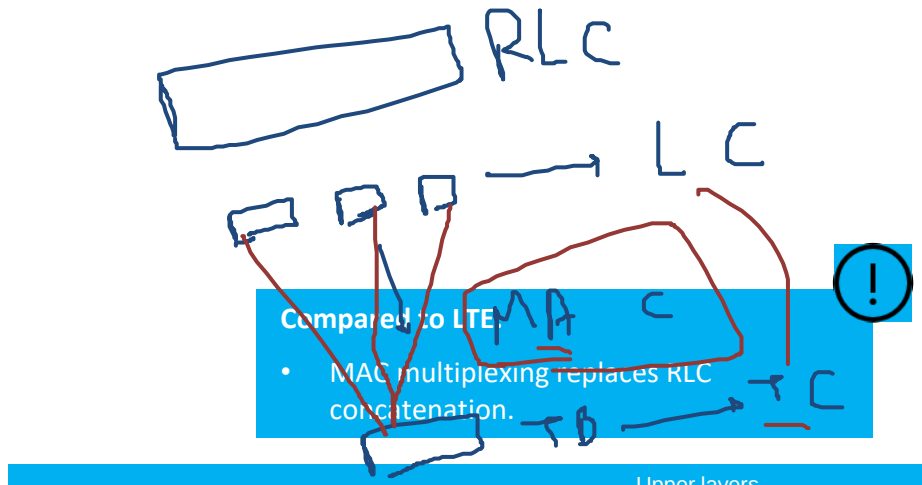
NEA0 – Null ciphering
NEA1 – SNOW 3G based
NEA2 – AES based
NEA3 – ZUC based



Medium Access Control(MAC)

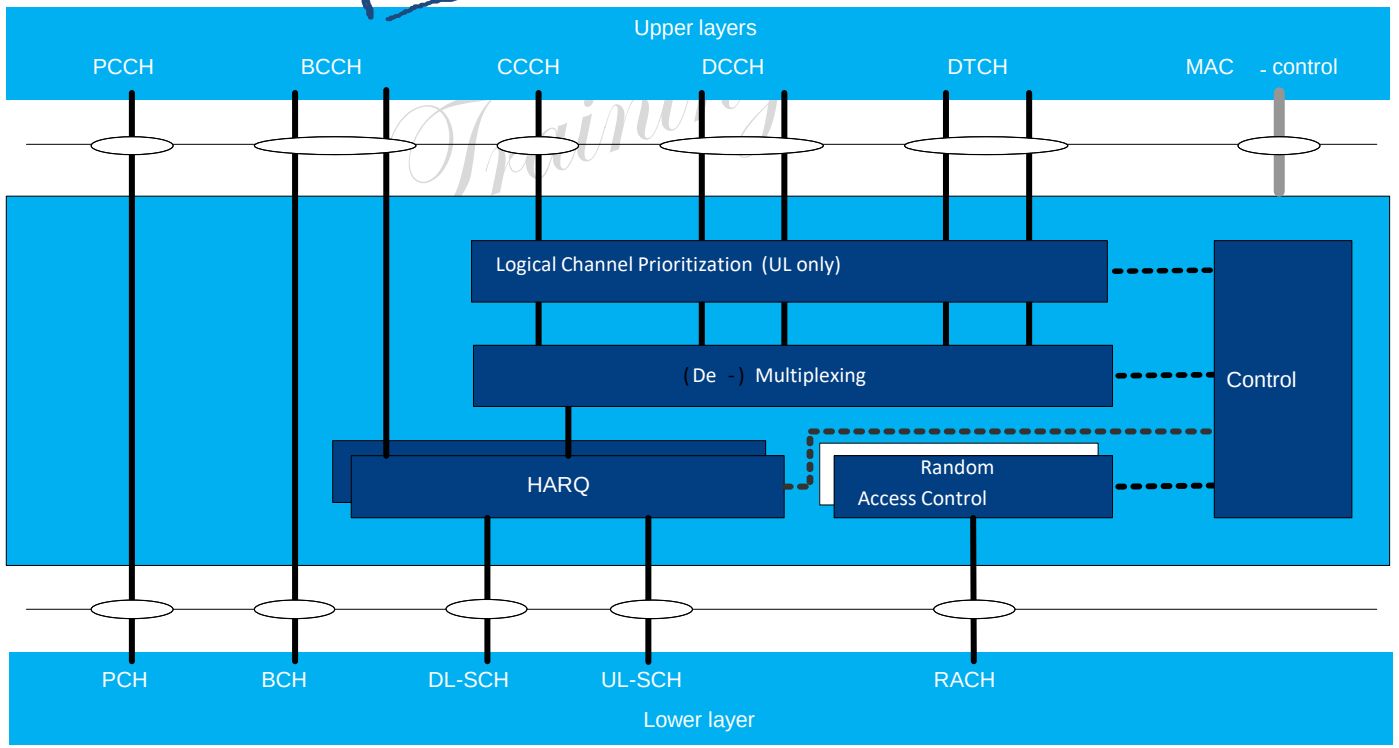
MAC Protocol Entity

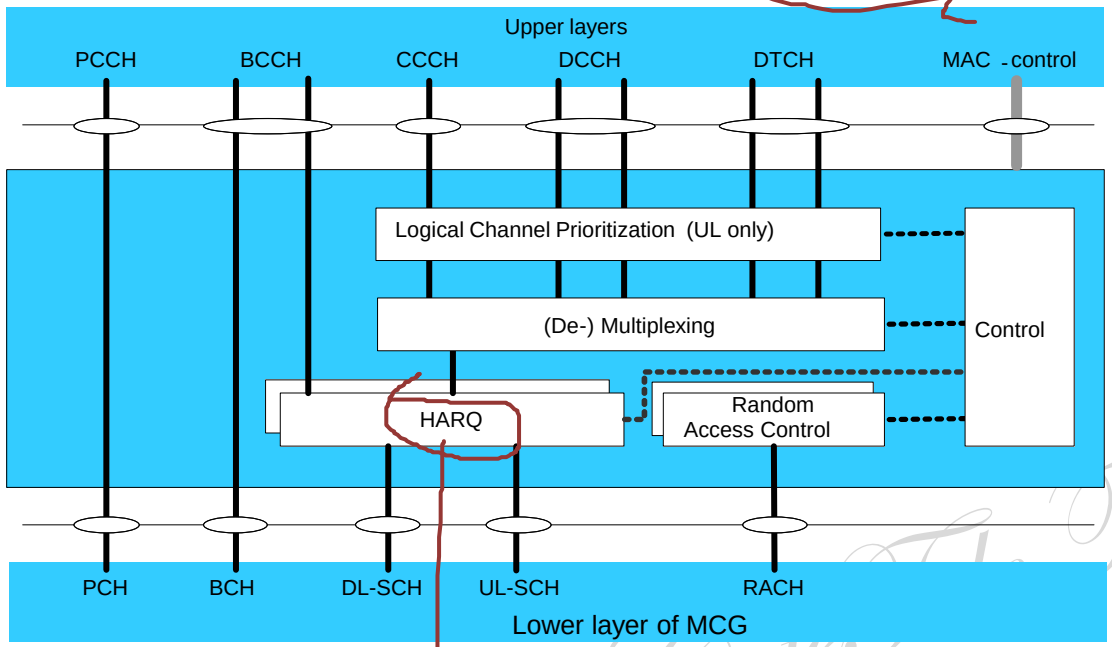
- **MAC Services**
  - Data Transfer
  - Radio resource allocation
- **Services expected from physical layer:**
  - data transfer services;
  - signalling of HARQ feedback;
  - signalling of Scheduling Request;
  - measurements (e.g. Channel Quality Indication (CQI)).
- **MAC Functions**
  - Mapping between logical channels and transport channels
  - Multiplexing of MAC SDUs
  - Demultiplexing of MAC SDUs
  - Scheduling information reporting
  - Error correction through HARQ
  - Logical channel prioritization

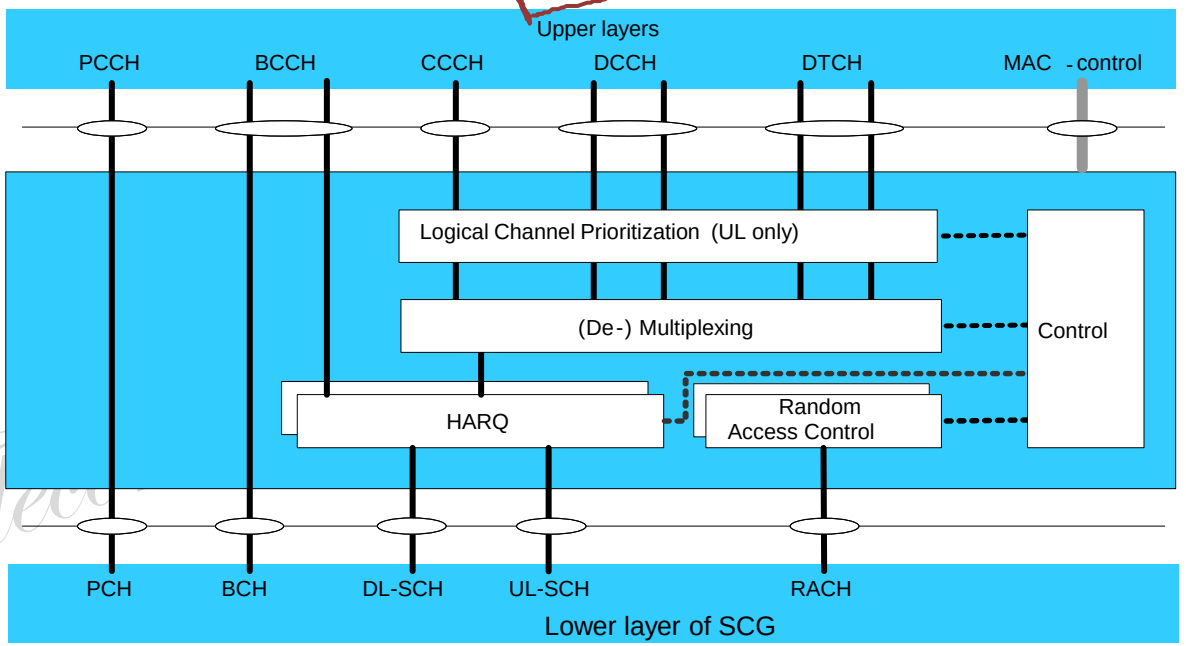


Compared to LTE:

- MAC multiplexing replaces RLC concatenation.







MAC structure overview with two MAC entities

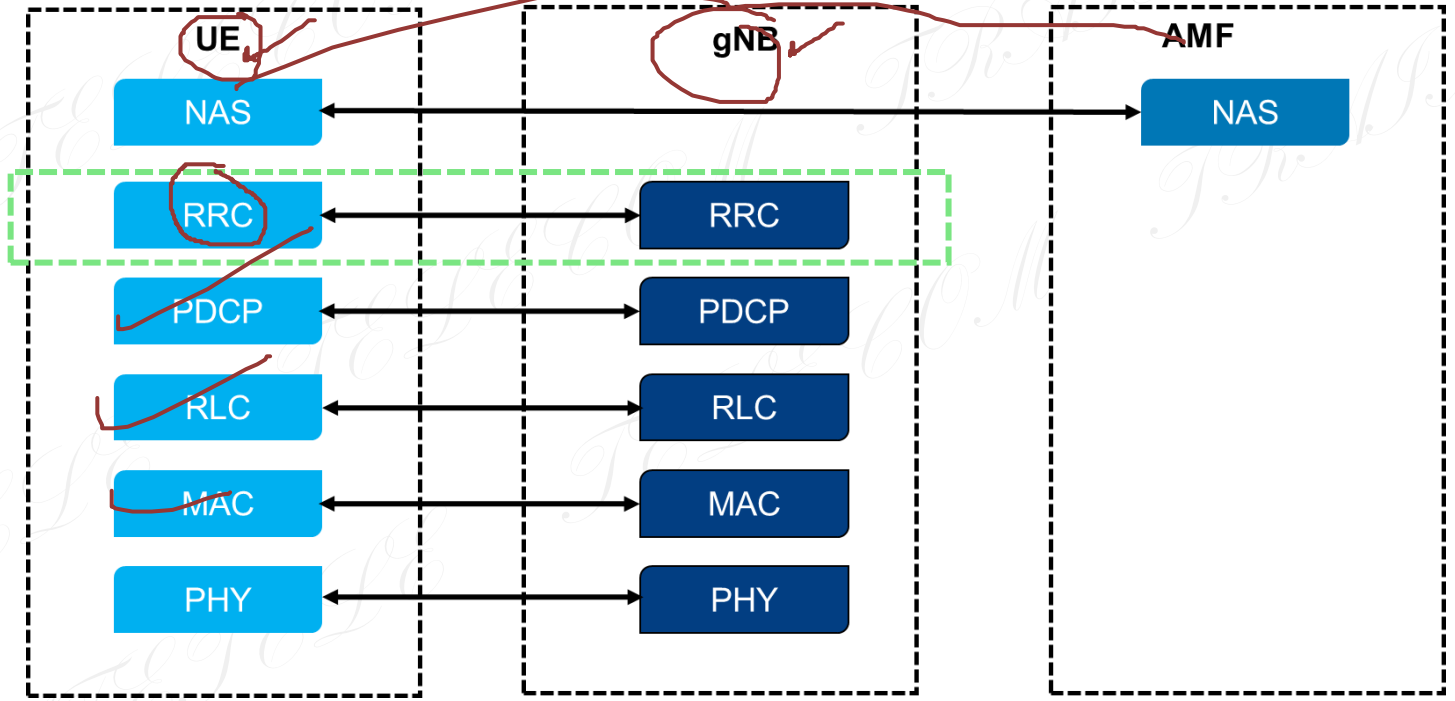
Radio Resource Control(RRC)

- Control Plane Radio Protocol Architecture
- RRC Functions
- UE states and state transitions
- UE's activities in each RRC State
- Signaling Radio Bearer

Control Plane Radio Protocol Architecture

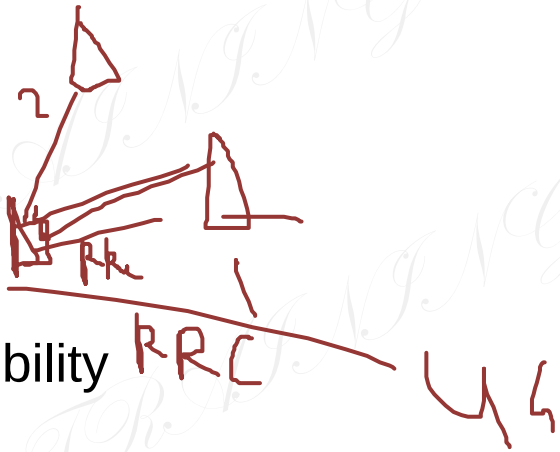
❖Control Plane

- RRC Function between UE and gNB
- Transferring of NAS information between UE and AMF
- NAS control Protocols is terminated in AMF on the network side



NAS: Non Access stratum
AMF: Access and Mobility Management function

RRC Functions(1/3)



❖Summary of RRC functions

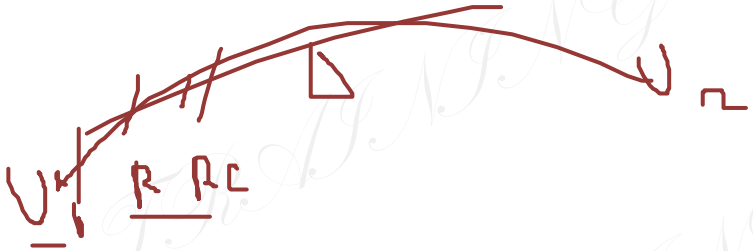
- Broadcast of system information
- RRC connection control & intra/inter-frequency mobility
- Inter-RAT mobility
- Measurement configuration and reporting
- Transfer of dedicated NAS information and etc.

❖Broadcast of system information

- NAS common information
- Information applicable for UEs in RRC_IDLE and RRC_INACTIVE
  - Cell (re-)selection parameters, neighbor cell information
- Information applicable for UEs in RRC_CONNECTED
  - Common channel configuration information
- ETWS/CMAS notification

- ETWS : Earthquake and Tsunami Warning System
- CMAS : Commercial Mobile Alert System

RRC Functions(2/3)



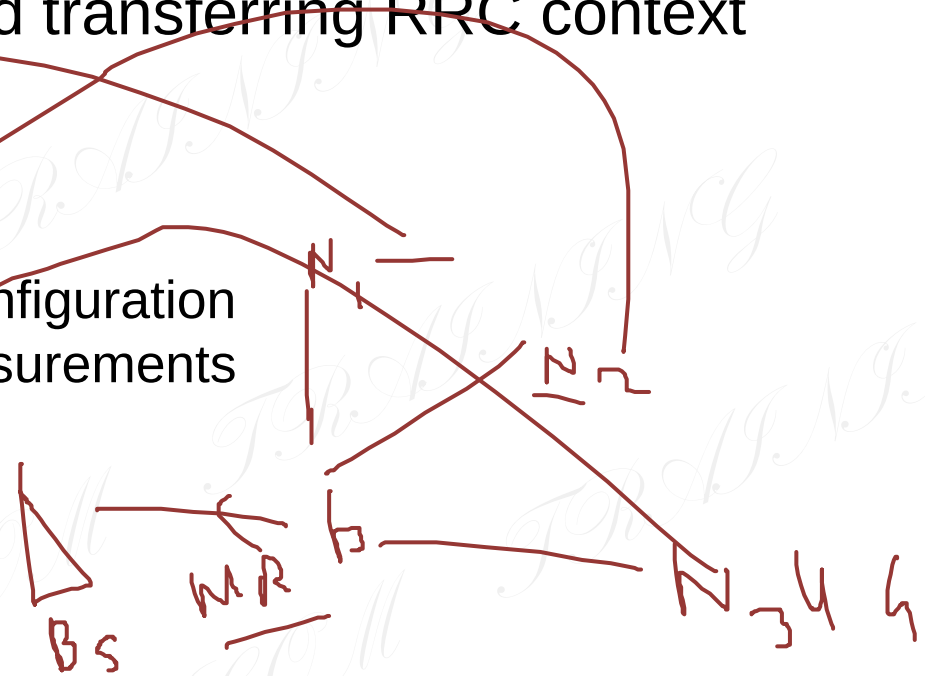
❖ RRC connection control

- Paging
- Establishment/modification/suspension/resumption/release of RRC connection and SRBs & DRBs
- Assignment/modification of UE identity (C-RNTI, I-RNTI, etc.)
- Initial configuration of AS integrity protection and AS ciphering
- RRC connection mobility (Intra-frequency & Inter-frequency handover)
- Radio configuration control
  - Assignment/modification of ARQ, HARQ and DRX configuration
- Dual Connectivity(DC) cell management
  - Change of PSCell, addition/modification/release of SCG cell(s)
- Carrier Aggregation(CA) cell management
  - Addition/modification/release of SCell(s)
- QoS control
  - Semi-persistent scheduling (SPS) configuration and grant configuration for DL and UL
  - Assignment/ modification of parameters for UL rate control in the UE
- Recovery from radio link failure

RRC Functions(3/3)

- Inter-RAT mobility including security activation and transferring RRC context information

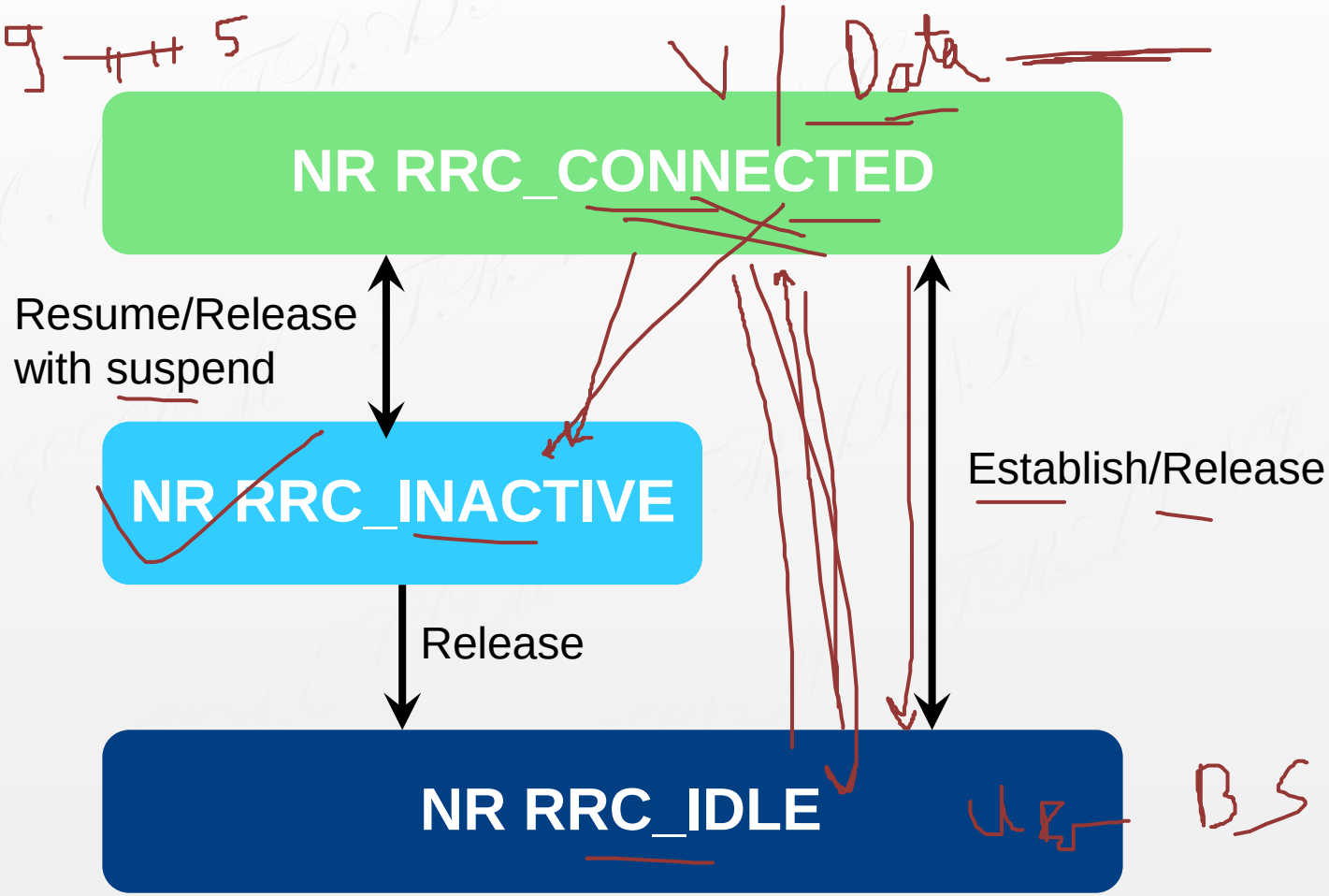
- Measurement configuration and reporting
  - Establishment/modification/release of measurement configuration
    - Intra-frequency, inter-frequency and inter-RAT measurements
  - Setup and release of measurement gaps
  - Measurement reporting



- Other functions
  - Generic protocol error handling
  - Transfer of dedicated NAS information and UE radio access capability information

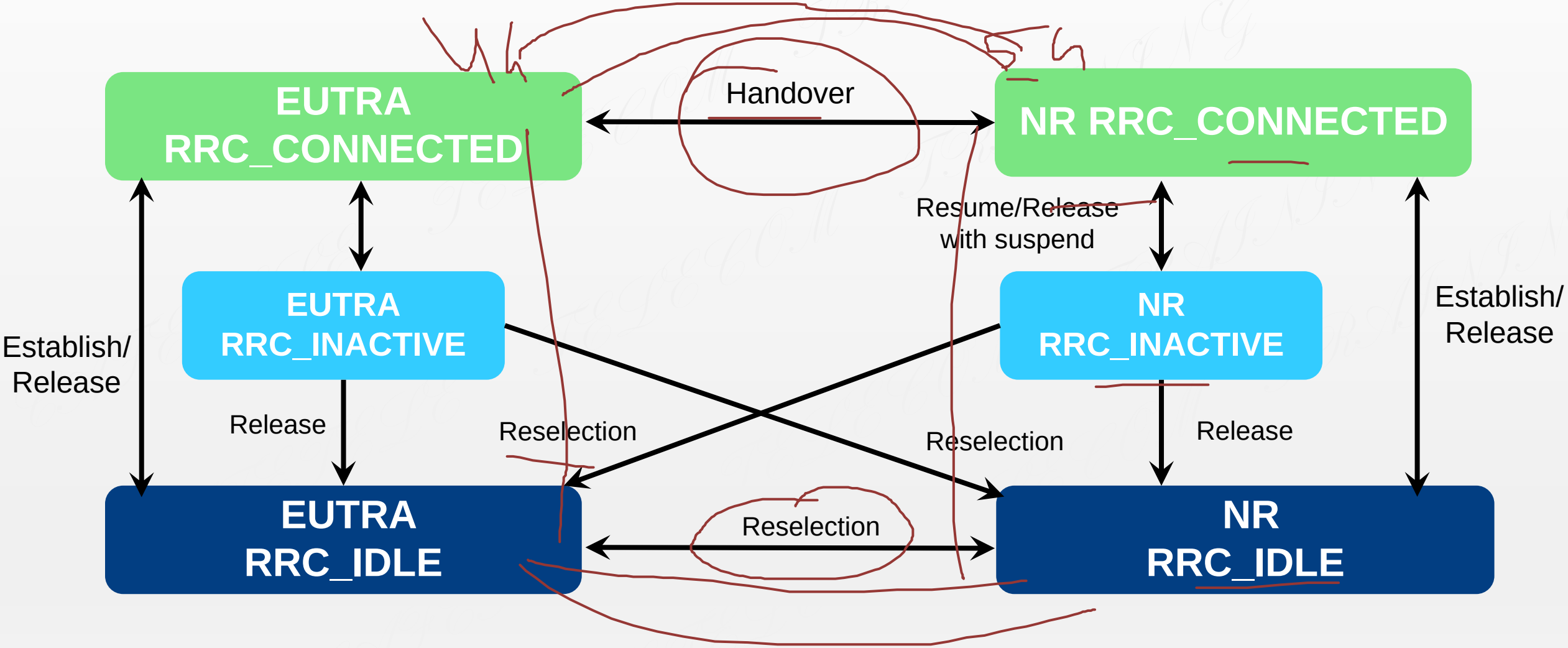
UE states and state transitions(SA)

- UE RRC States in NR
  - RRC_IDLE
  - RRC_INACTIVE
  - RRC_CONNECTED



UE RRC state and state transitions in NR

UE state machine and state transitions between NR/5GC, E-UTRA/EPC and EUTRA/5GC

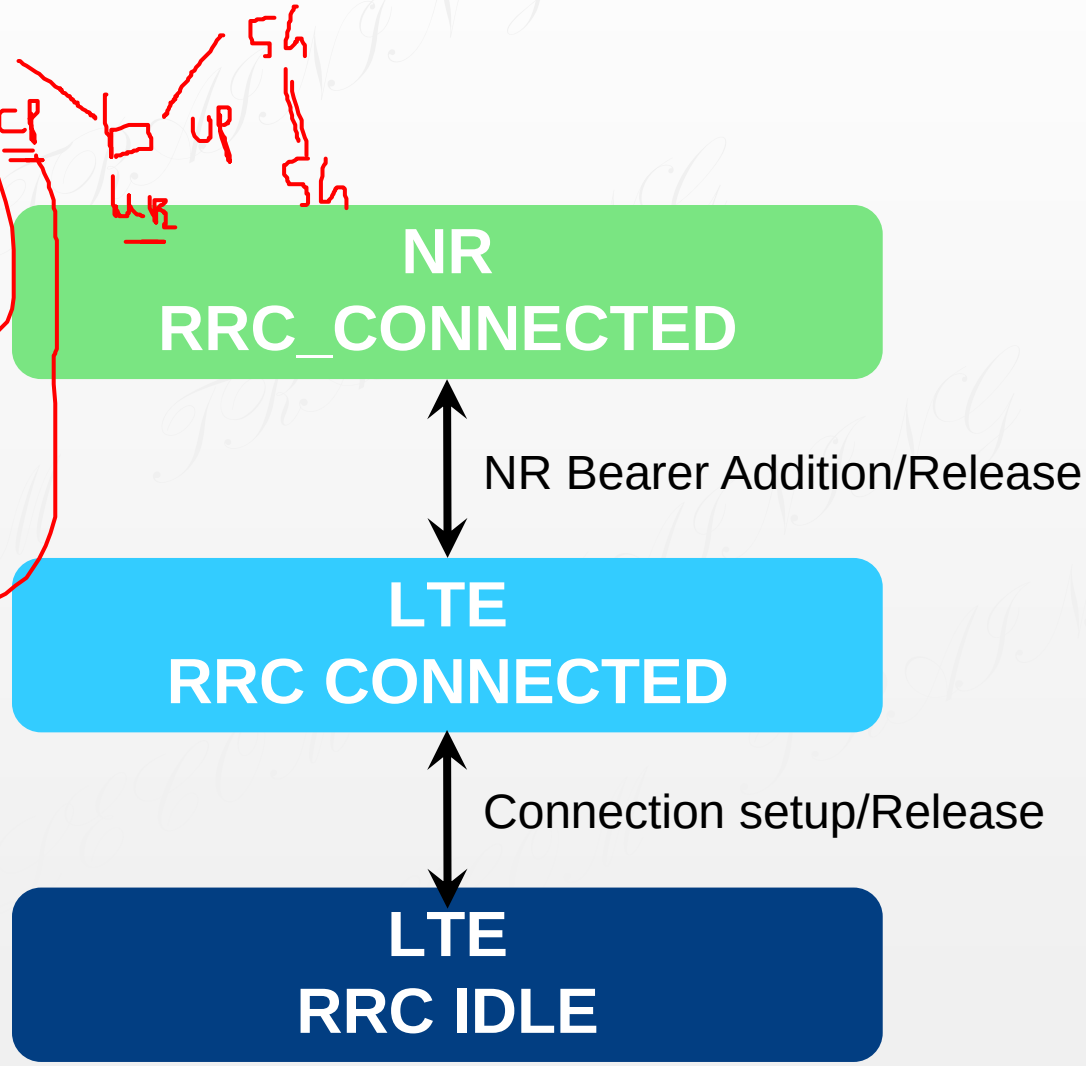


5G NR RRC State NSA

UE has dual connectivity with LTE and NR and supports mobility activities as handover and PSCell change

Measurement report of NR cell can be sent Via LTE SRB

UE Camping in a LTE cell, still needs search and measure NR and Shows NR icon in the phone screen



What is the RADIUS protocol?

Remote Authentication Dial-In User Service (RADIUS) is a networking protocol that exchanges authentication, authorization, and accounting (AAA) data between a client and a server.

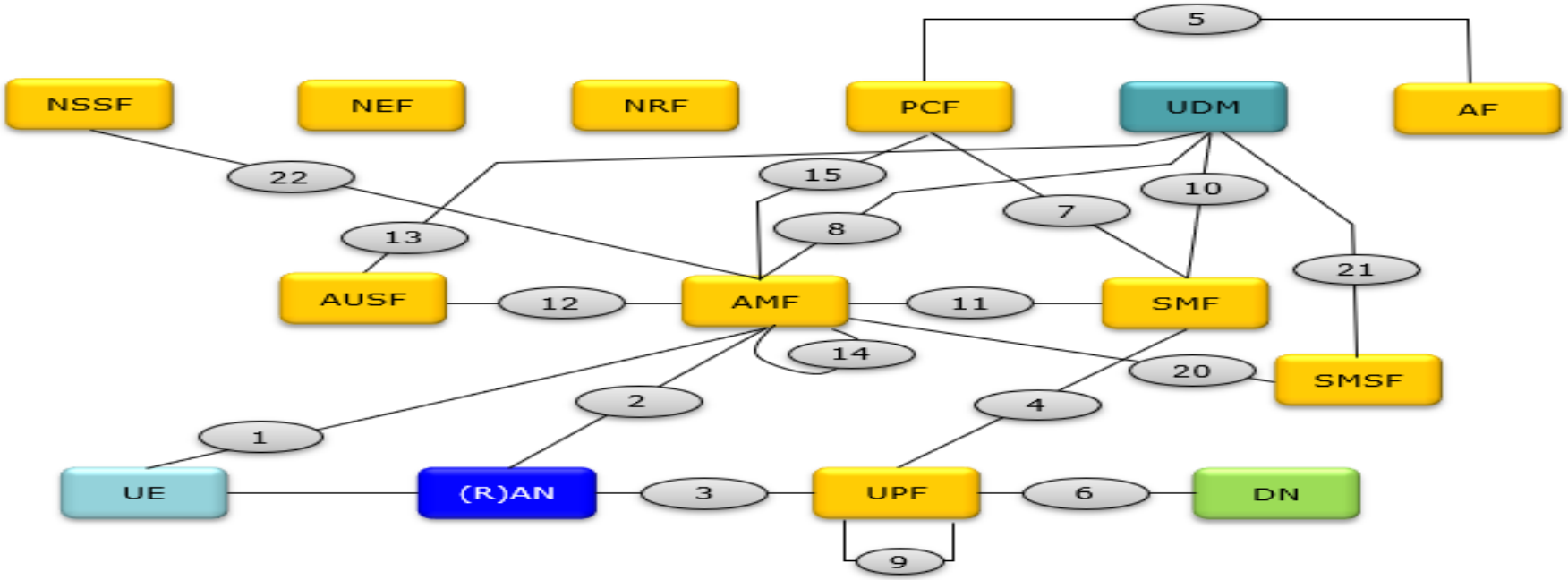
What is the Diameter protocol?

Diameter is a networking protocol that exchanges authentication, authorization, and accounting (AAA) data between two parties. Unlike RADIUS, which only allows a client to deliver a request to the server, Diameter also allows sending a request from a server to a client.

Interfaces and Network Functions

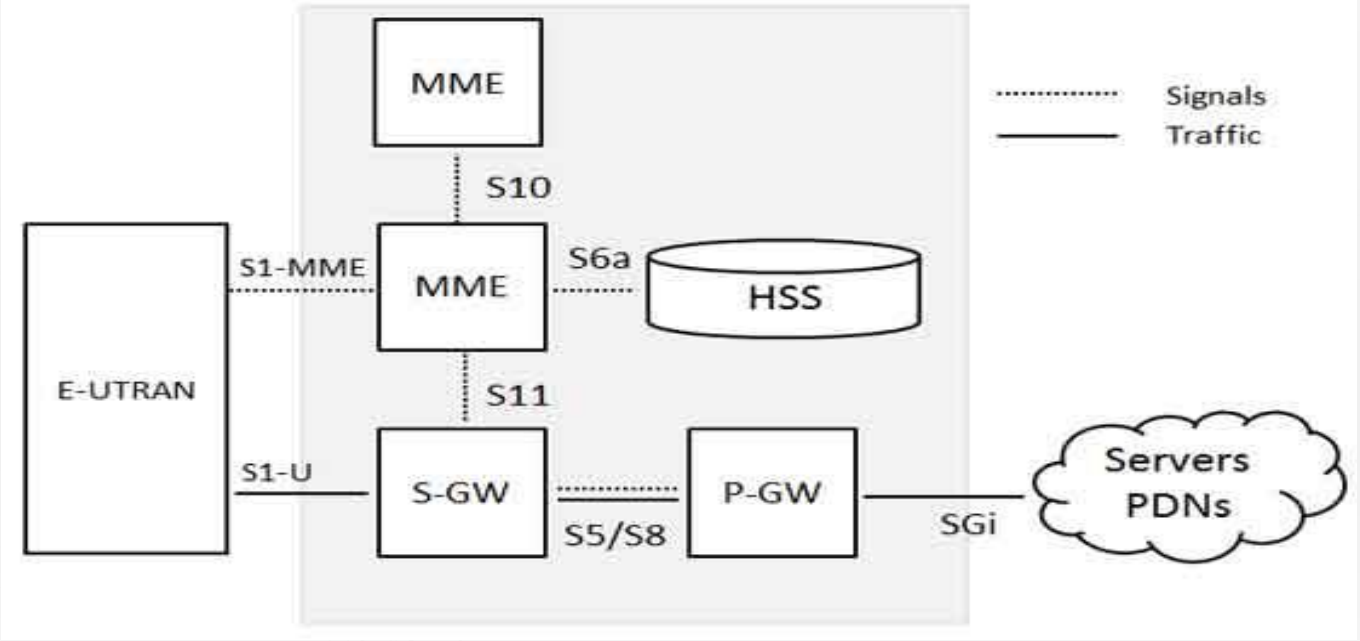
N1 and S1

In the context of 5G networking, N1 and S1 modes refer to different ways a user equipment (UE) can access the network, with specific implications for the kind of network architecture the UE is interfacing with.



- N1 Mode: In N1 mode, the UE has access to the 5G core network (5GC) via the 5G access network. This mode is indicative of a successful 5GC attach, which means the UE is connected to the 5G network and is able to utilize its services

- S1 Mode: When a UE is capable of S1 mode, it implies that the UE has a single usage setting that applies to both the 5G system (5GS) and the evolved packet system (EPS). In this mode, the UE is recognized as having a successful EPS attach. This mode is important for ensuring backward compatibility with the LTE network and for situations where the UE might be moving between areas that have different generations of network technology



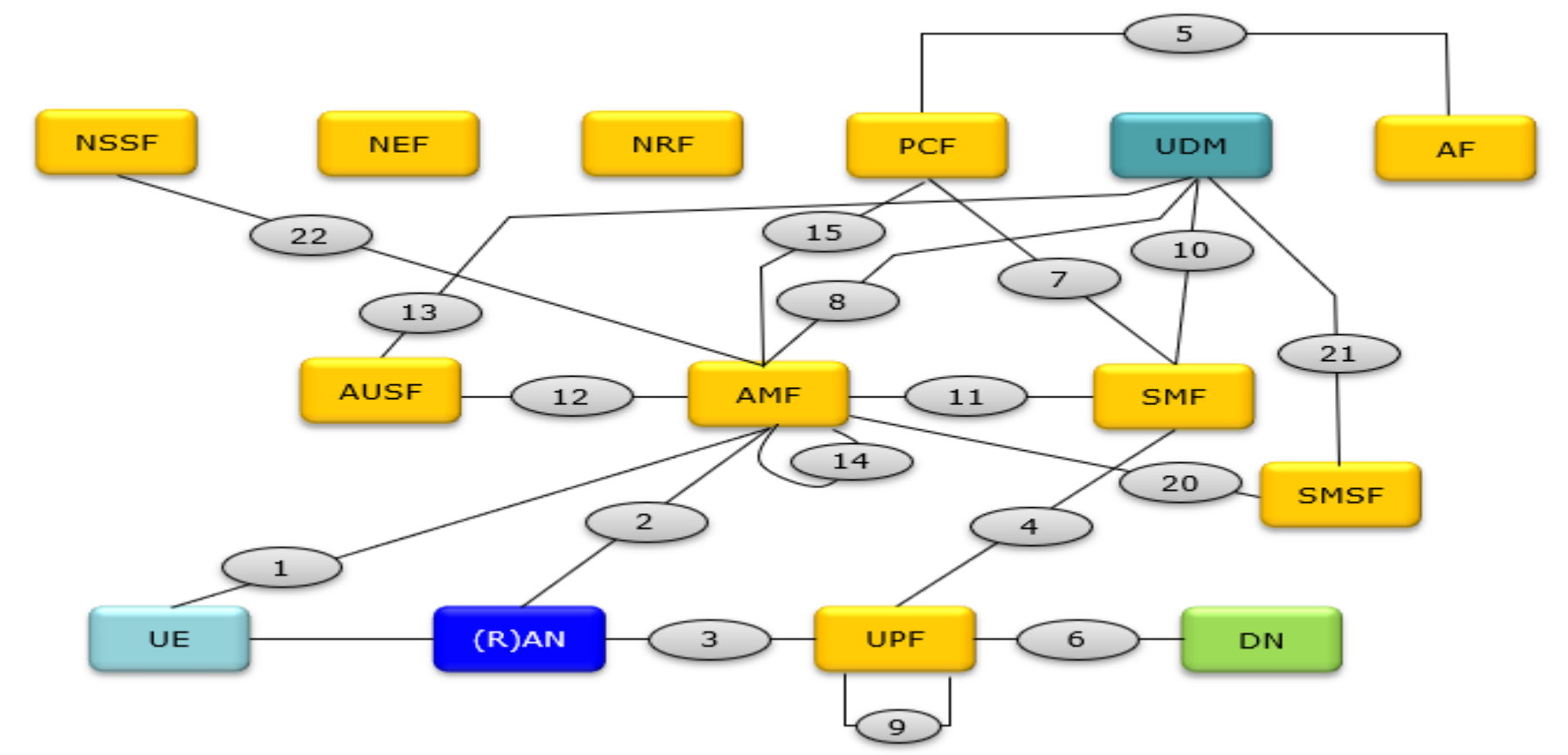
- N1 mode refers to Standalone mode with direct connection between 5G RAN and 5G Core. S1 mode refers to Non-Standalone with connection between 5G RAN and 4G EPC core.

- In N1 mode, the NG interface is used between RAN and 5GC. In S1 mode, existing 4G S1 interface is reused between RAN and EPC.

- N1 mode allows full 5G core network features like network slicing, advanced QoS, unified authentication, etc. S1 mode has limitations of 4G core.
- The 5G core network functions like AMF, SMF, UPF are utilized in N1 mode.

- In S1 mode, 4G elements like MME, SGW, PGW are still used.
- N1 mode simplifies the architecture with a common core for different access types. S1 mode retains the overlapping 4G and 5G cores.
- N1 mode requires deploying the new 5G core first. S1 mode allows introducing 5G NR with existing 4G core.

N1 Interface, N2 Interface, N8 Interface, N22 Interface, N26 Interface



What is N1 Interface

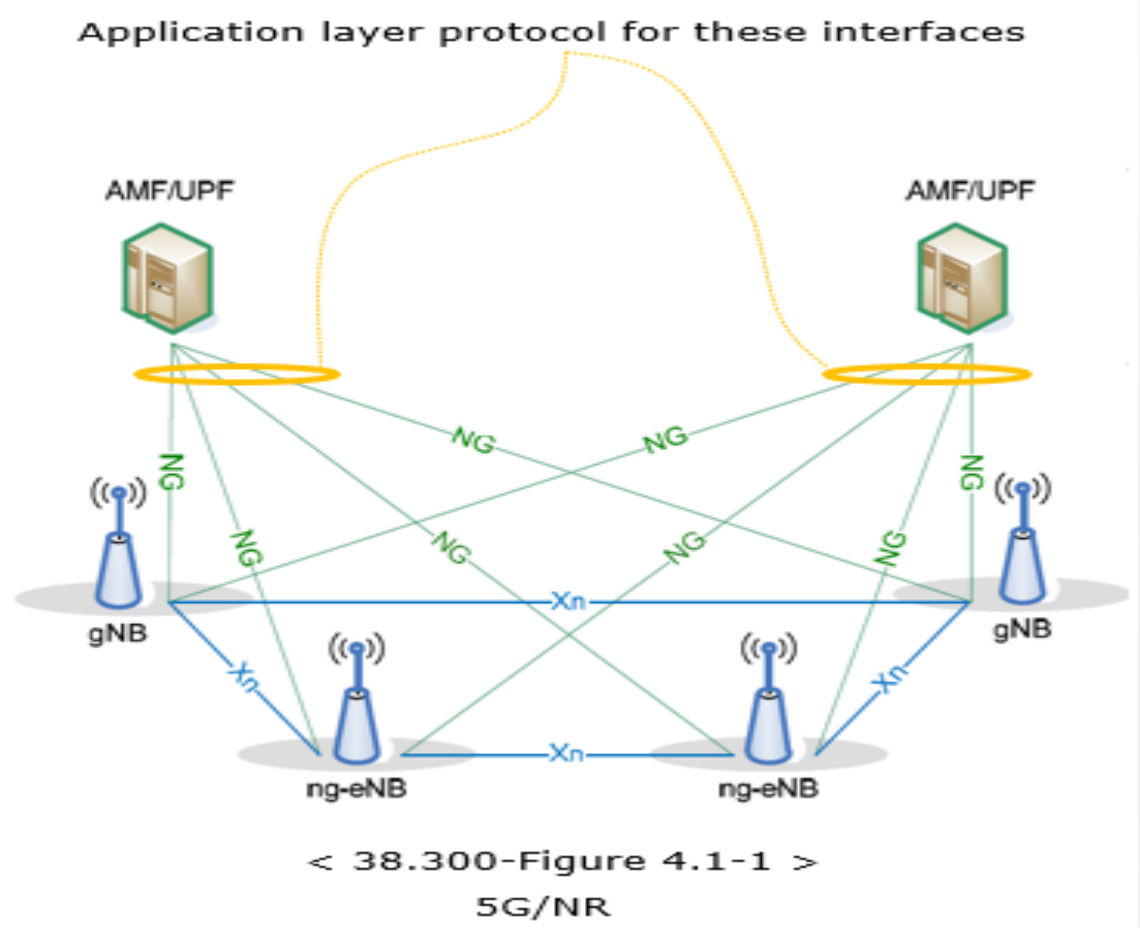
N1 is the interface between UE and AMF
N1 represents the combined path UE <--> Access Network and Access Network <--> AMF
The Access Network can be a 3GPP based Most of NAS signaling is going through N1

NR CORE - N8

N8 is the interface between AMF and UDM. It is mainly used when AMF needs some user(subscriber) data from UDM and plays important role especially during the registration process

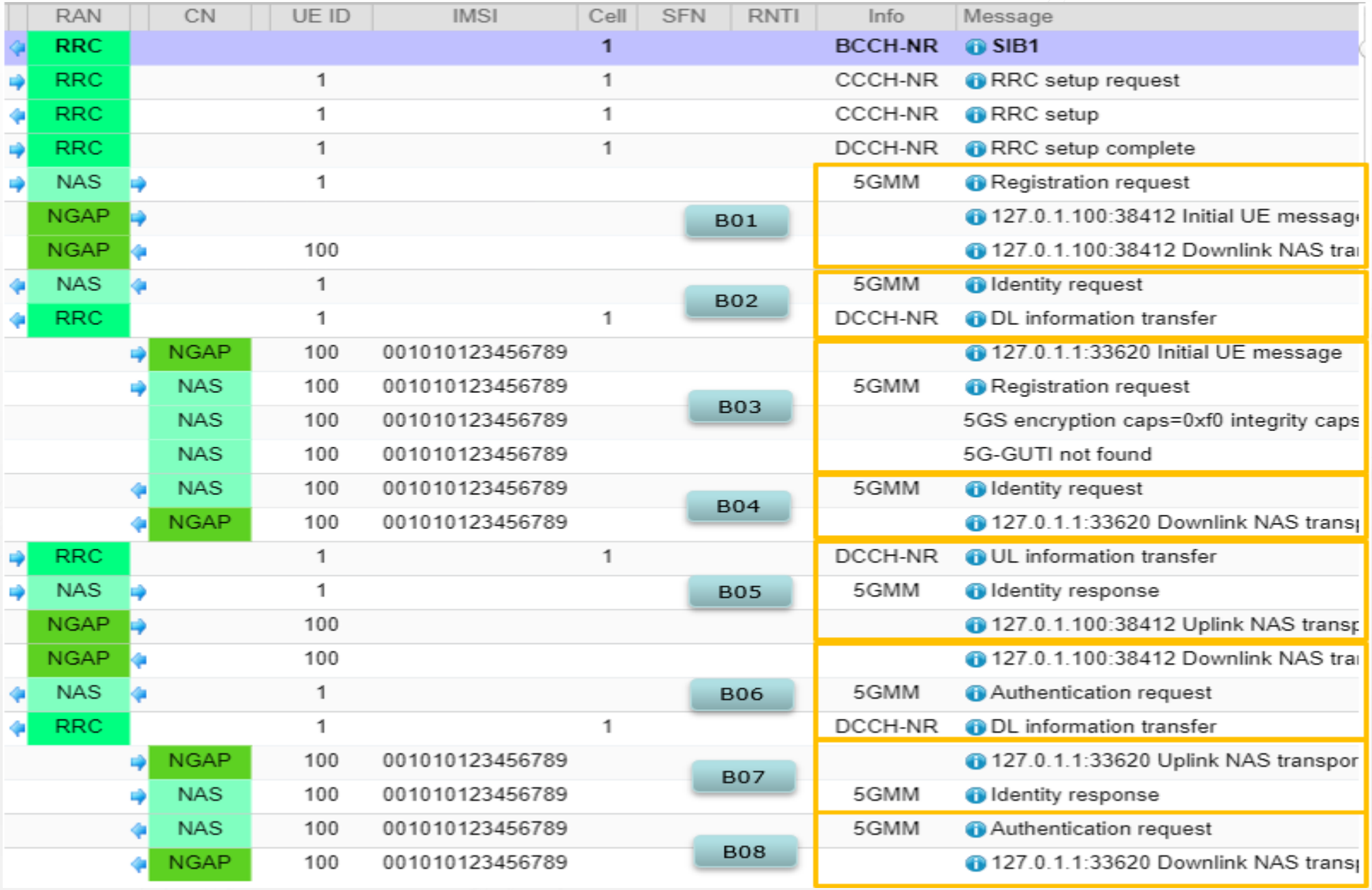
NGAP / N2 Interface

NGAP is the protocol(an Application Layer Protocol) being used in the communication between between gNB and AMF as illustrated below.

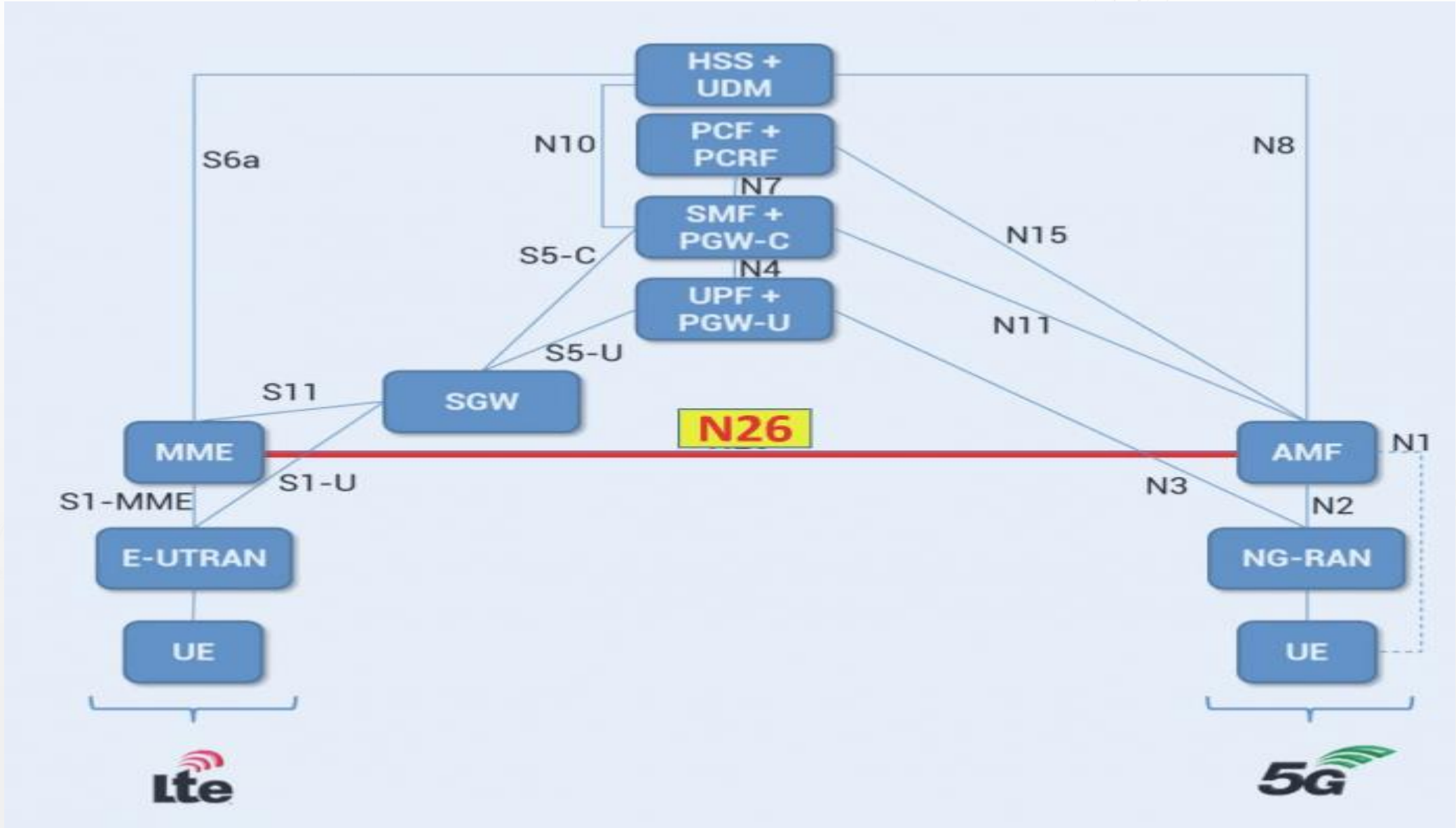


Signaling (Message flow between gNB and AMF) - N2 Interface

The signaling message reaching to AMF through N2 interfaces will be conveyed to various other core network components via corresponding interfaces.



RAN	CN	UE ID	IMSI	Cell	SFN	RNTI	Info	Message
RRC				1			BCCH-NR	SIB1
RRC		1		1			CCCH-NR	RRC setup request
RRC		1		1			CCCH-NR	RRC setup
RRC		1		1			DCCH-NR	RRC setup complete
NAS		1					5GMM	Registration request
NGAP					B01			127.0.1.100:38412 Initial UE messag
NGAP		100						127.0.1.100:38412 Downlink NAS tra
NAS		1			B02		5GMM	Identity request
RRC		1		1			DCCH-NR	DL information transfer
	NGAP	100	001010123456789					127.0.1.1:33620 Initial UE message
	NAS	100	001010123456789		B03		5GMM	Registration request
	NAS	100	001010123456789					5GS encryption caps=0xf0 integrity caps
	NAS	100	001010123456789					5G-GUTI not found
	NAS	100	001010123456789		B04		5GMM	Identity request
	NGAP	100	001010123456789					127.0.1.1:33620 Downlink NAS transp
RRC		1		1			DCCH-NR	UL information transfer
NAS		1			B05		5GMM	Identity response
NGAP		100						127.0.1.100:38412 Uplink NAS transp
NGAP		100						127.0.1.100:38412 Downlink NAS tra
NAS		1			B06		5GMM	Authentication request
RRC		1		1			DCCH-NR	DL information transfer
	NGAP	100	001010123456789		B07			127.0.1.1:33620 Uplink NAS transpor
	NAS	100	001010123456789				5GMM	Identity response
	NAS	100	001010123456789		B08		5GMM	Authentication request
	NGAP	100	001010123456789					127.0.1.1:33620 Downlink NAS transp


HSS + UDM
PCF + PCRF
SMF + PGW-C
UPF + PGW-U
SGW
MME
E-UTRAN
UE
AMF
NG-RAN
UE
S6a
N10
N8
N7
N15
S5-C
N4
N11
S5-U
S11
N26
N1
S1-U
N3
S1-MME
N2
Lte
5G

N26 is an inter-CN interface between AMF and MME in order to enable interworking between the 5G core and EPC. Support of N26 interface in the network is optional. Interworking procedures using N26 interface enable the exchange of MM and SM states between the source and target networks. Handover procedures are supported through N26 interface.

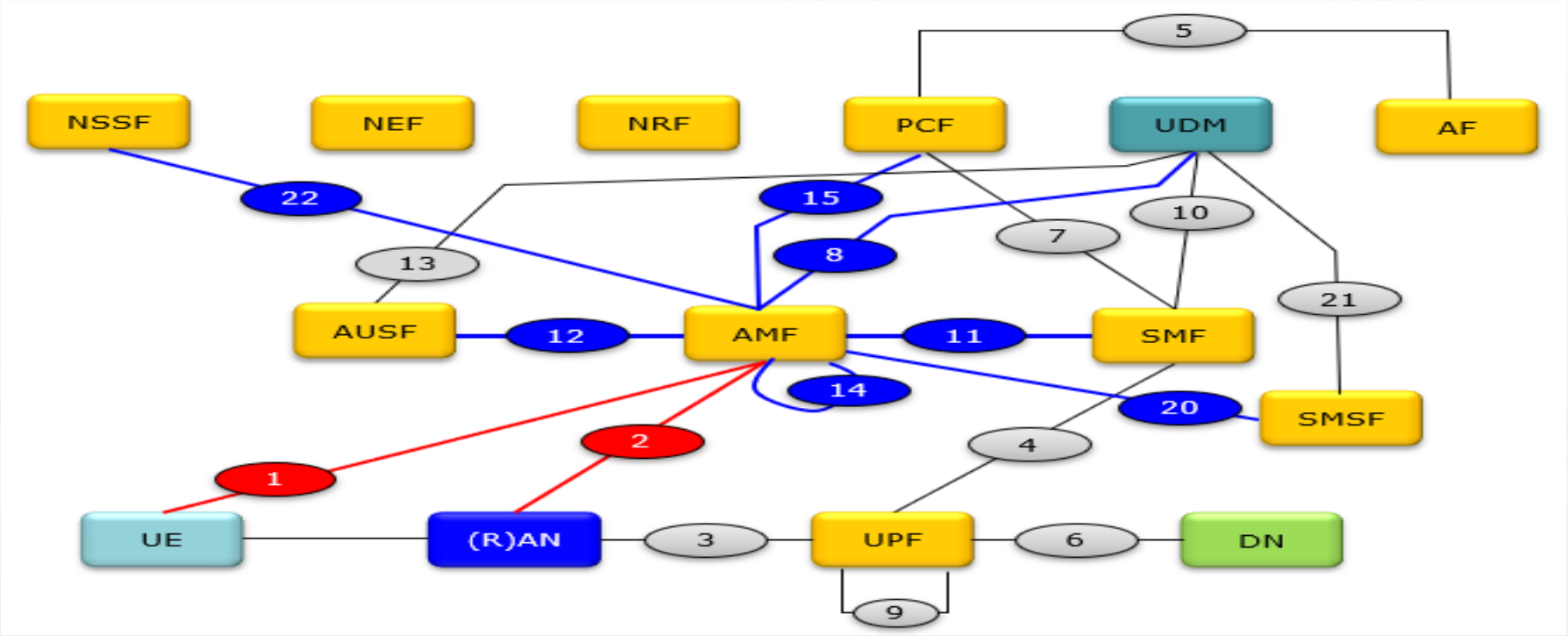
The support for N26 interface between AMF in 5GC and MME in EPC is required to enable seamless session continuity for inter-system handover which will be critical for voice services.

Network Functions: AMF, NRF, N22 - NSSF

The Access and Mobility Management Function (AMF)

one of the control plane network functions (NF) of the 5G core network (5GC). The 5G AMF, is an evolution of 4G MME, continuing with the Control Plane and User Plane Separation, and with further simplifications like moving the Sessions Management functions to the SMF and, providing common SBA interfaces.

NR CORE - AMF plays the most critical(central) roles in 5G core network. Simply put, AMF is a central control box or central hub of the whole 5G core network.



The Major role of AMF is to handle NAS message from UE. This NAS message would mostly comes from RAN (gNB) but theoretically it can come from other Non 3GPP components. As shown below, the communication between AMF and RAN is going through N1 interface

AMF Functionality/Services

Registration Management:
- Allows UE to register and deregister with 5G network
- Handles initial registration to authorize UE and create UE context
- Manages periodic registration updates to verify UE status

Connection Management:
- Establishes and releases control plane N1 signaling connections with UE
- Manages transitions between CM-Idle and CM-Connected states

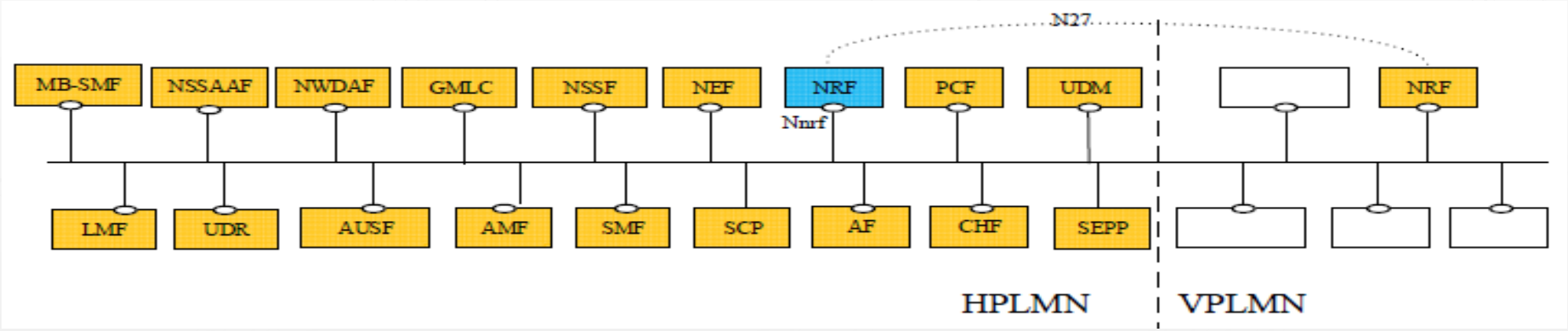
Reachability Management:
- Ensures UE is reachable for mobile-terminated connections
- Uses paging to trigger idle UEs to establish connections

Mobility Management:
- Maintains knowledge of UE location within network
- Manages mobility tracking area updates
- Handles Xn handovers between gNB base stations

Access Authentication:
- Authenticates UEs during initial registration and periodic updates
- Verifies UE identity and validity of SIM credentials
- Authorizes UE access to 5G services and network

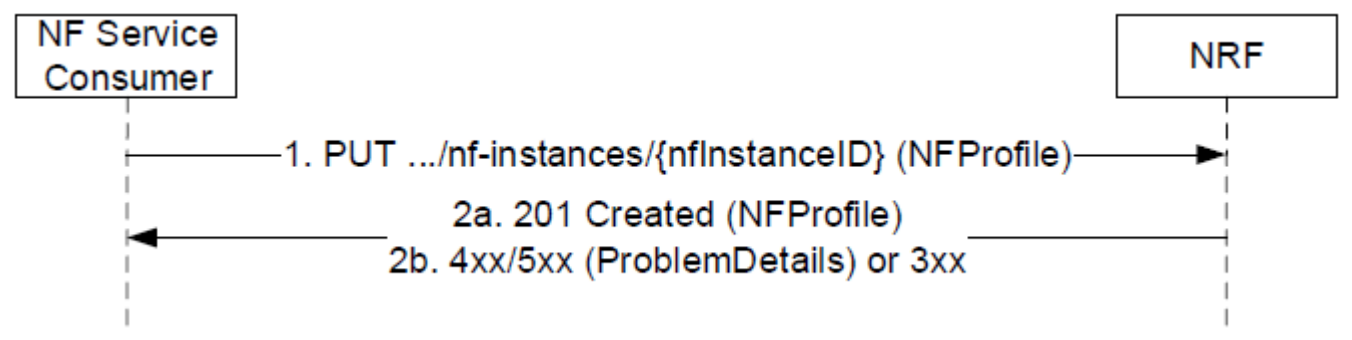
NR CORE - NRF

NRF stands for Network function Repository Function. Simply put, it works as a central registration center (registra) for all the Core Network Components. As shown in the following diagram, NRF has connected to all the 5G Core



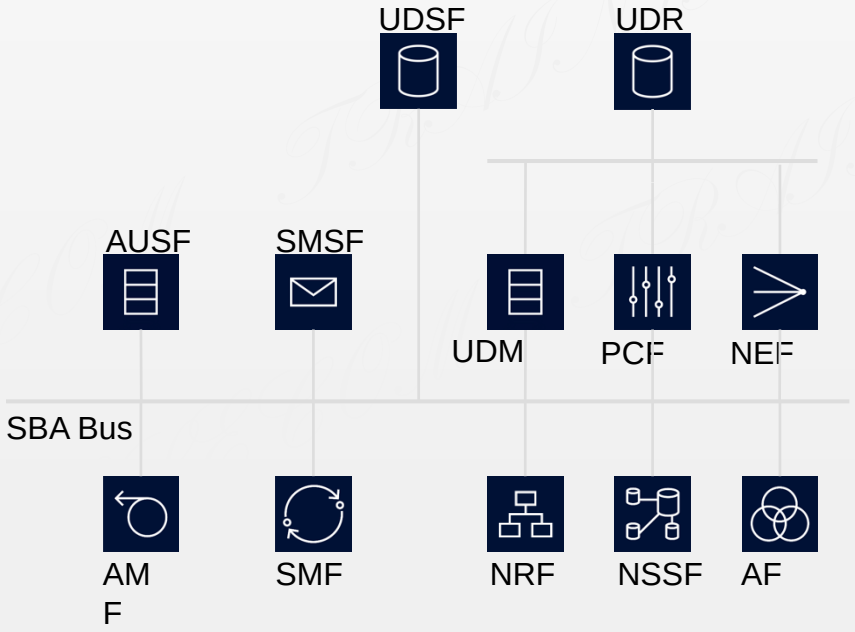
Since NRF is connected almost every components (Network Functions) and provide various services to all of them. Descriptions on this NF(Network Function) can be complicated

NF Registration to NRF



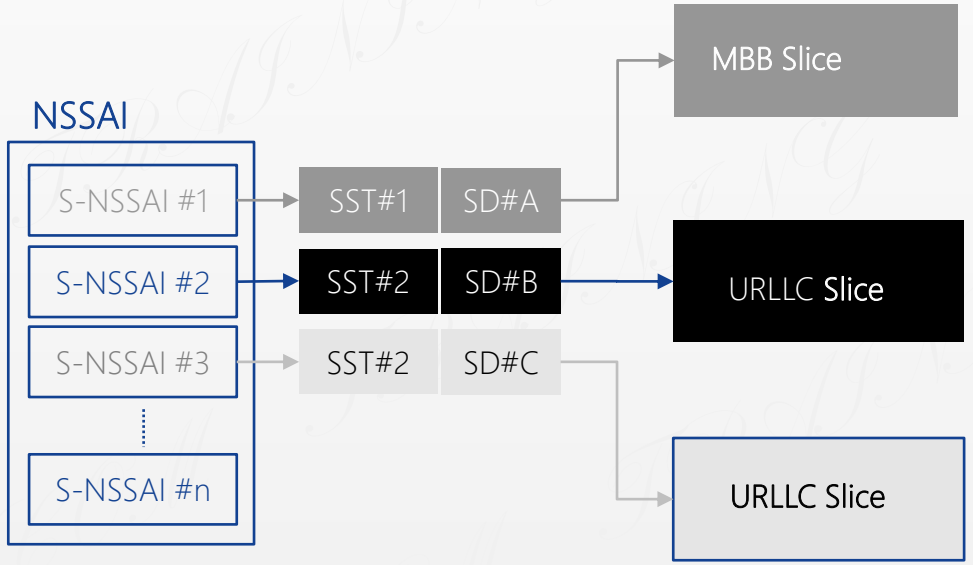
Network Slice Selection Function (NSSF):

- It determines the allowed slices a UE can use
- It determines the AMF to be used to serve the UE, or, based on configuration, a list of candidate AMF(s), possibly by querying the NRF.
- And it selects the set of network slice instances serving the UE



NSSAI:	• Network Slice Selection Assistance Information • The NSSAI is a collection of up to 8 S-NSSAIs
S-NSSAI: Single NSSAI	• S-NSSAI : Single Network Slice Selection Assistance information • It identifies a Network Slice.
S-NSSAI is comprised of:	• A **Slice/Service type (SST),** which refers to the expected Network Slice behavior in terms of features and services • A **Slice Differentiator (SD).** which is optional information that complements the Slice/Service type(s) to allow further differentiation for selecting a Network Slice from the potentially multiple Network Slices that all comply with the indicated Slice/Service type

S-NSSAI = Slice/Service type (SST) + Slice Differentiator (SD)



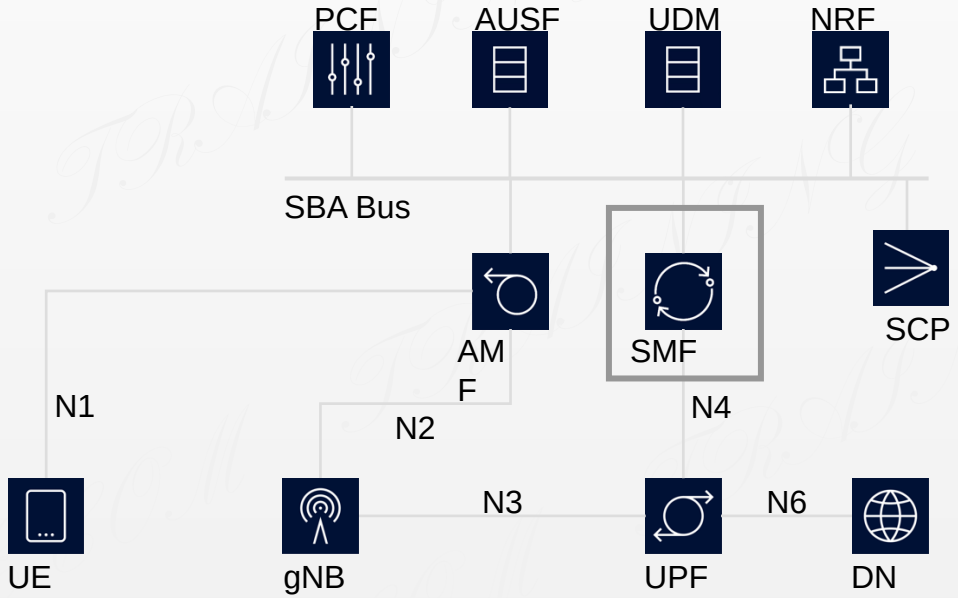
TS 23.501 Standardized SST table

Session Management Function

Handles establishment, modification and release of PDU sessions. Interacts with the access network via the AMF

Performs UPF selection (via NRF) and control (via N4). Handles IP address management

Interfaces with the Charging and Policy functions. Determines the SSC mode of a PDU session

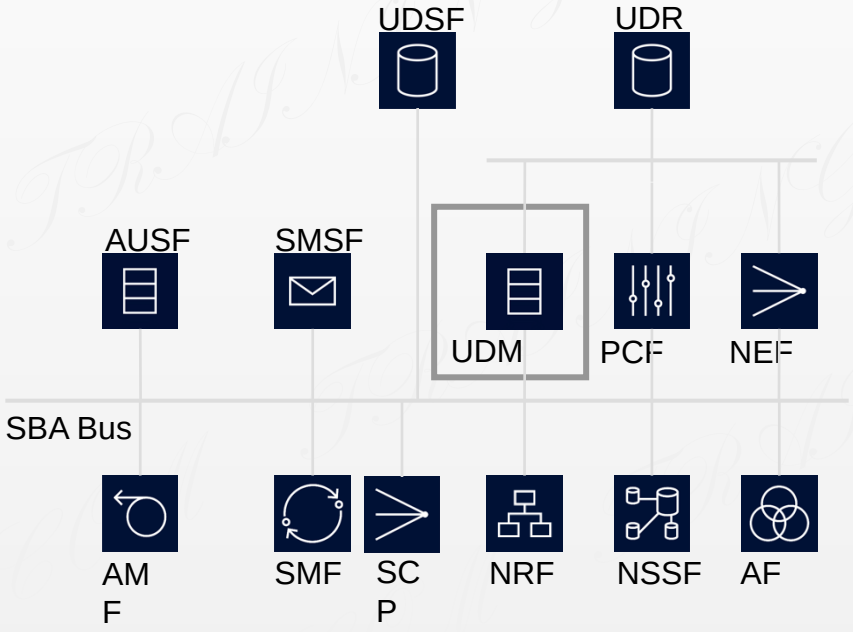


Unified Data Management

UDM manages subscriber data and profiles

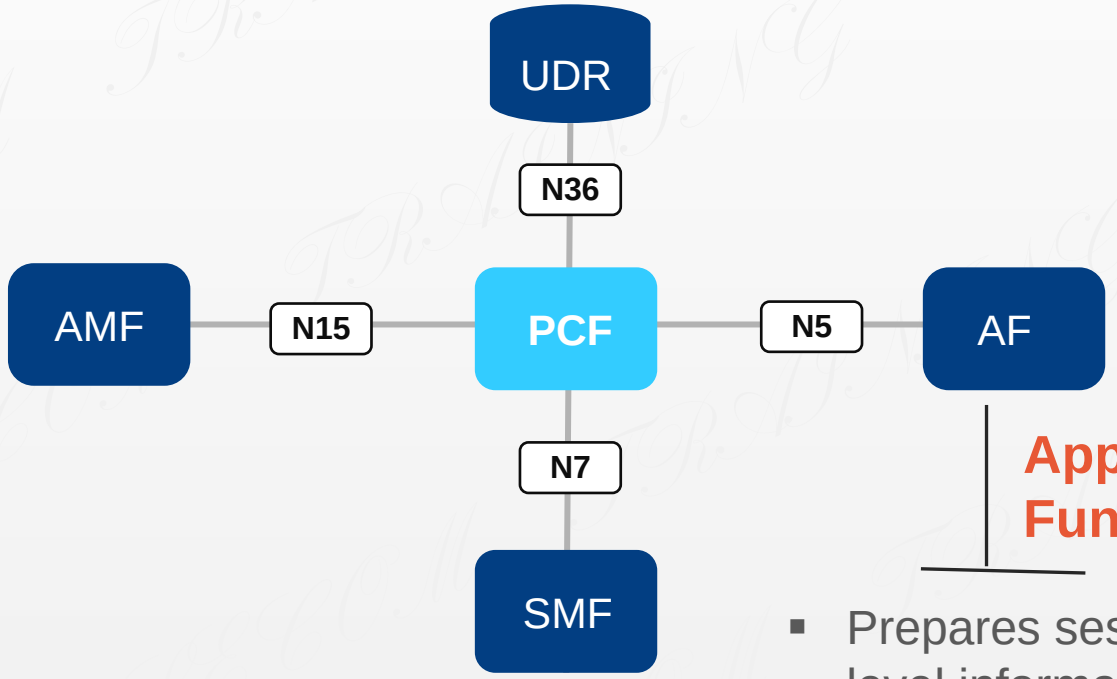
Similar to the home subscriber server (HSS) or home location register (HLR

UDM uses subscription data and authentication data that may be stored in UDR



Policy Control Function (PCF)

- Policy Decisions
- Policy Rule Distribution
- Access to subscriber information
- Interaction with PCF



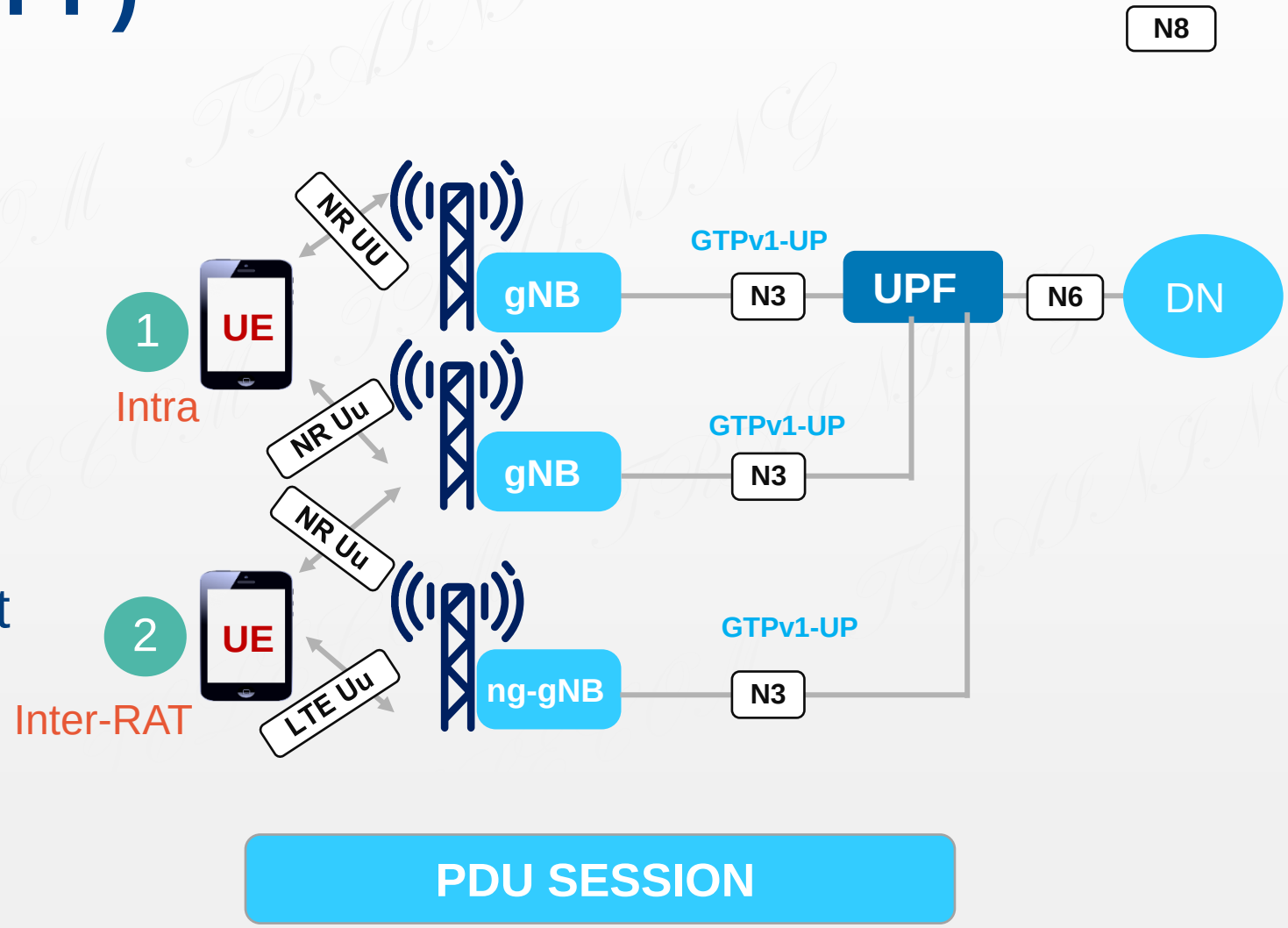
Application Function (AF)

- Prepares session level information to the PCF to support the policy decisions

- Based on operator deployment, Application Functions considered to be trusted by the operator can be allowed to interact directly with relevant Network Functions.

User plane function (UPF)

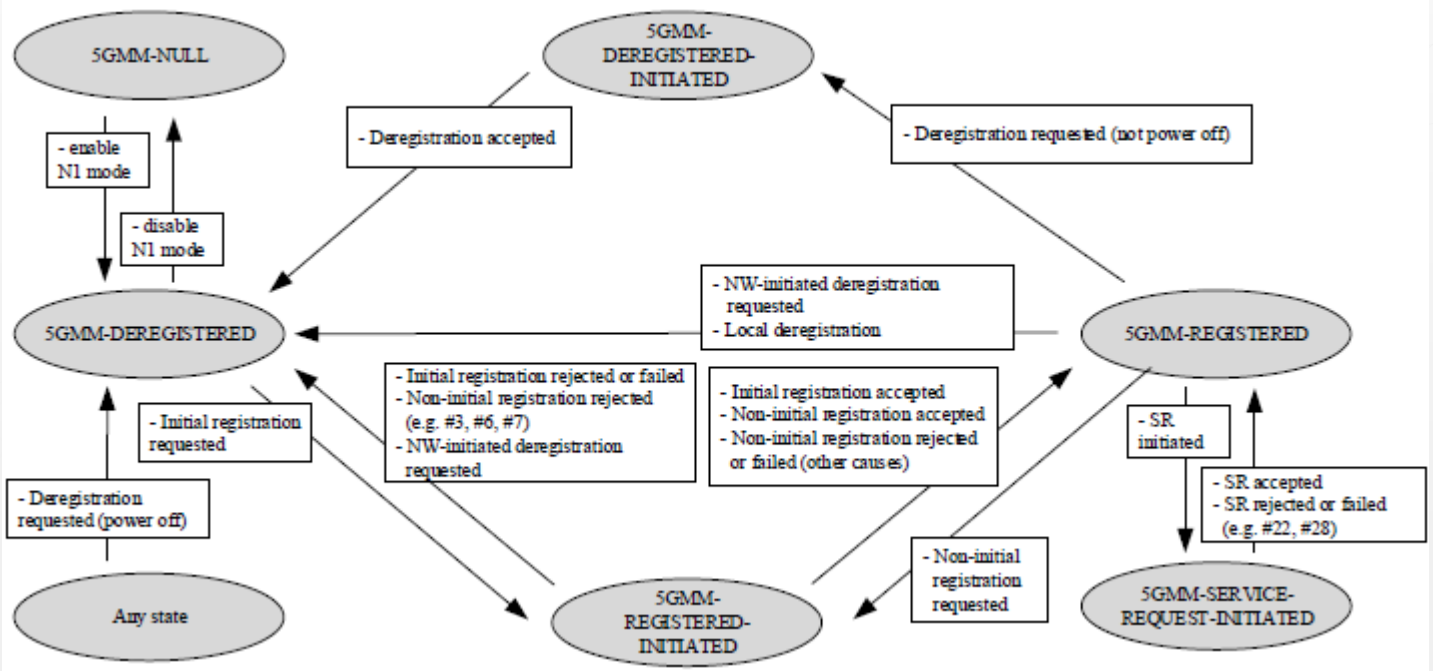
- Anchor point for Intra-/Inter-RAT mobility
- External PDU Session point of interconnect to Data Network.
- Packet routing & forwarding
- QoS and Policy Rule Enforcement
- Traffic usage reporting
- Data Buffering



5GMM(5G Mobility Management)

5G Mobile Management is involved mainly in NAS registration process and in terms of corenetwork interface point of view, it is mostly associated with N1/N2 interface.

5GMM Statemachine



5GMM-NULL: This state represents the initial condition when the UE is powered on or reset. In this state, 5GS services are disabled in the UE. No 5GS mobility management function shall be performed in this state. The UE is not registered to any 5G network, and no context is stored in the network for the UE. The UE is not reachable for mobile-terminated services.

5GMM-DEREGISTERED: In this state, the UE is not registered to any 5G network. No 5GMM context has been established and the UE location is unknown to the network and hence it is unreachable by a network. In order to establish a 5GMM context, the UE shall start the initial registration procedure. It is either switched off, out of coverage, or has been deregistered from the network for some reason. The UE is not reachable for mobile-terminated services, and no context is stored in the network for the UE

5GMM-DEREGISTERED-INITIATED: This state indicates that the UE has initiated the deregistration process but has not yet completed it. The UE is in the process of exchanging messages with the network to complete the deregistration.

5GMM-REGISTERED-INITIATED: In this state, the UE has initiated the registration process but has not yet completed it. The UE is in the process of exchanging messages with the network to complete the registration.

5GMM-REGISTERED: This state indicates that the UE has successfully registered with a 5G network. In this state, the UE can receive mobile-terminated services, and the network maintains context information for the UE. This state implies that the UE has successfully completed the registration process and can now utilize network services.

5GMM-SERVICE-REQUEST-INITIATED: In this state, the UE has initiated a service request to the network to establish a connection. This typically occurs when the UE needs to access specific network services or resources (e.g., to initiate a data session or a voice call). The UE remains in this state until the service request is either granted or rejected by the network.

5GSM(5G Session Management)

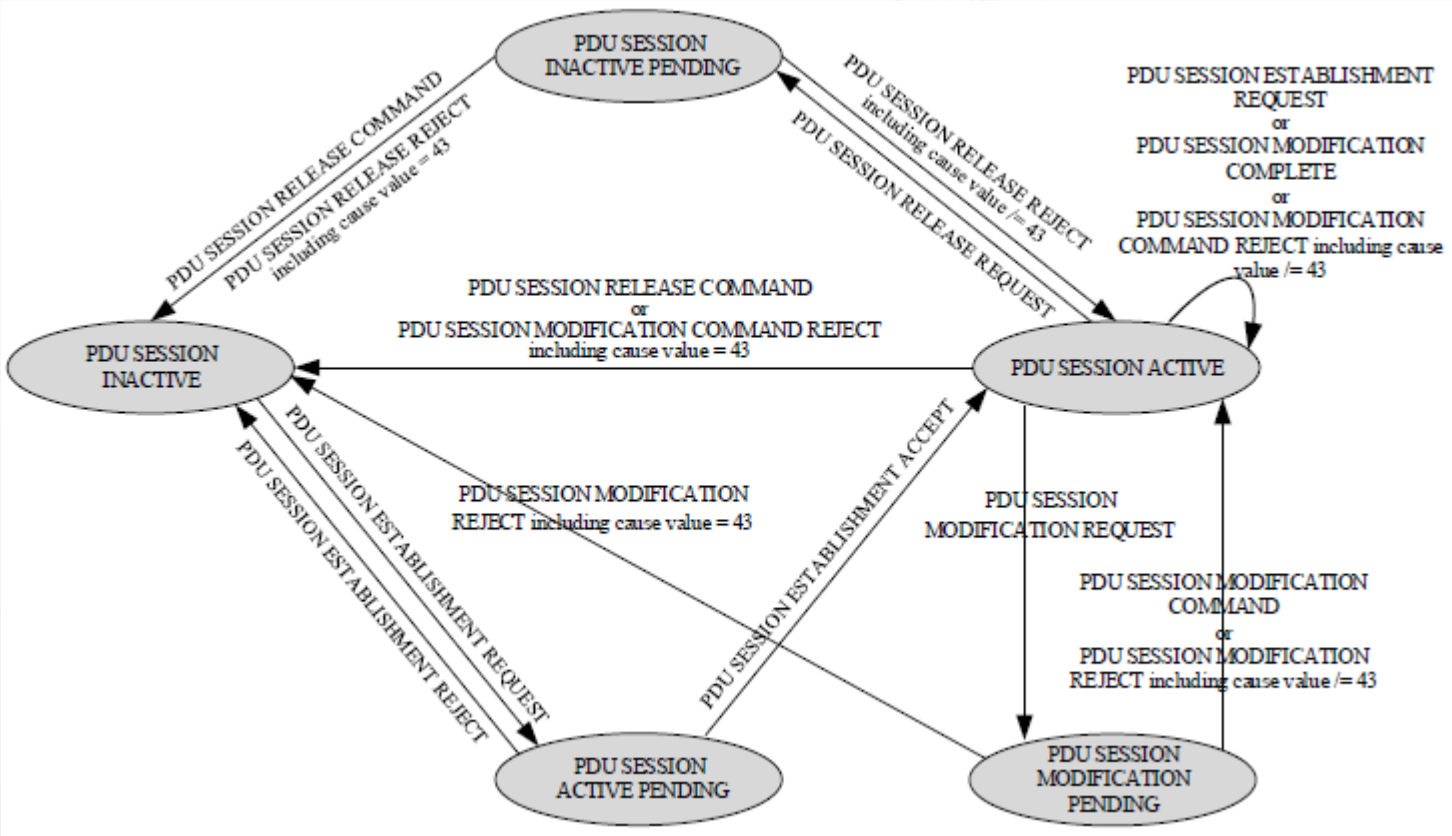
5GSM is a layer in core network that handles all the procedures for PDN. According to 24.501 - 6 Elementary procedures for 5GS session management, The main function of the 5GSM sublayer is to support the PDU session handling in the UE and in the SMF (transferred via the AMF).

Overall Functions of 5GSM

Overall description of 5GSM is well described in 24.501 - 6.1.1 as follows :
The 5GSM comprises procedures for:
the authentication and authorization, establishment, modification and release of PDU sessions; and
request for performing handover of an existing PDU session between 3GPP access and non-3GPP access, or to transfer an existing PDN connection in the EPS to the 5GS.

Each PDU session represents a PDU session established between the UE and an SMF. PDU sessions can remain established even if the radio and network resources constituting the corresponding PDU session between the UE and the SMF are temporarily released.

5GSM Statemachine



PDU Session Handling in UE

PDU SESSION INACTIVE : This is the state where the PDU session is not active, meaning there's no ongoing data transmission for this session.
Followings are transition to other states:
To PDU SESSION ACTIVE PENDING: Triggered by "PDU SESSION ESTABLISHMENT REQUEST".
PDU SESSION ACTIVE PENDING : This state indicates that the PDU session is in the process of becoming active.

Followings are transition to other states:
To PDU SESSION ACTIVE: Triggered by "PDU SESSION ESTABLISHMENT ACCEPT"
To PDU SESSION INACTIVE: Triggered by "PDU SESSION ESTABLISHMENT REJECT"

" PDU SESSION ACTIVE : The PDU session is active and data transmission is possible in this state.

Followings are transition to other states:
To PDU SESSION INACTIVE: Triggered by "PDU SESSION RELEASE COMMAND".
To PDU SESSION INACTIVE PENDING: Triggered by "PDU SESSION RELEASE REQUEST".
To PDU SESSION MODIFICATION PENDING: Triggered by "PDU SESSION MODIFICATION REQUEST"
Self-looping transition: Triggered by PDU SESSION ESTABLISHMENT REQUEST or PDU SESSION MODIFICATION COMPLETE

PDU SESSION INACTIVE PENDING : This state indicates that the PDU session is in the process of transitioning to an inactive status.

Followings are transition to other states:
To PDU SESSION INACTIVE: Triggered by PDU SESSION RELEASE COMMAND or "PDU SESSION RELEASE REJECT

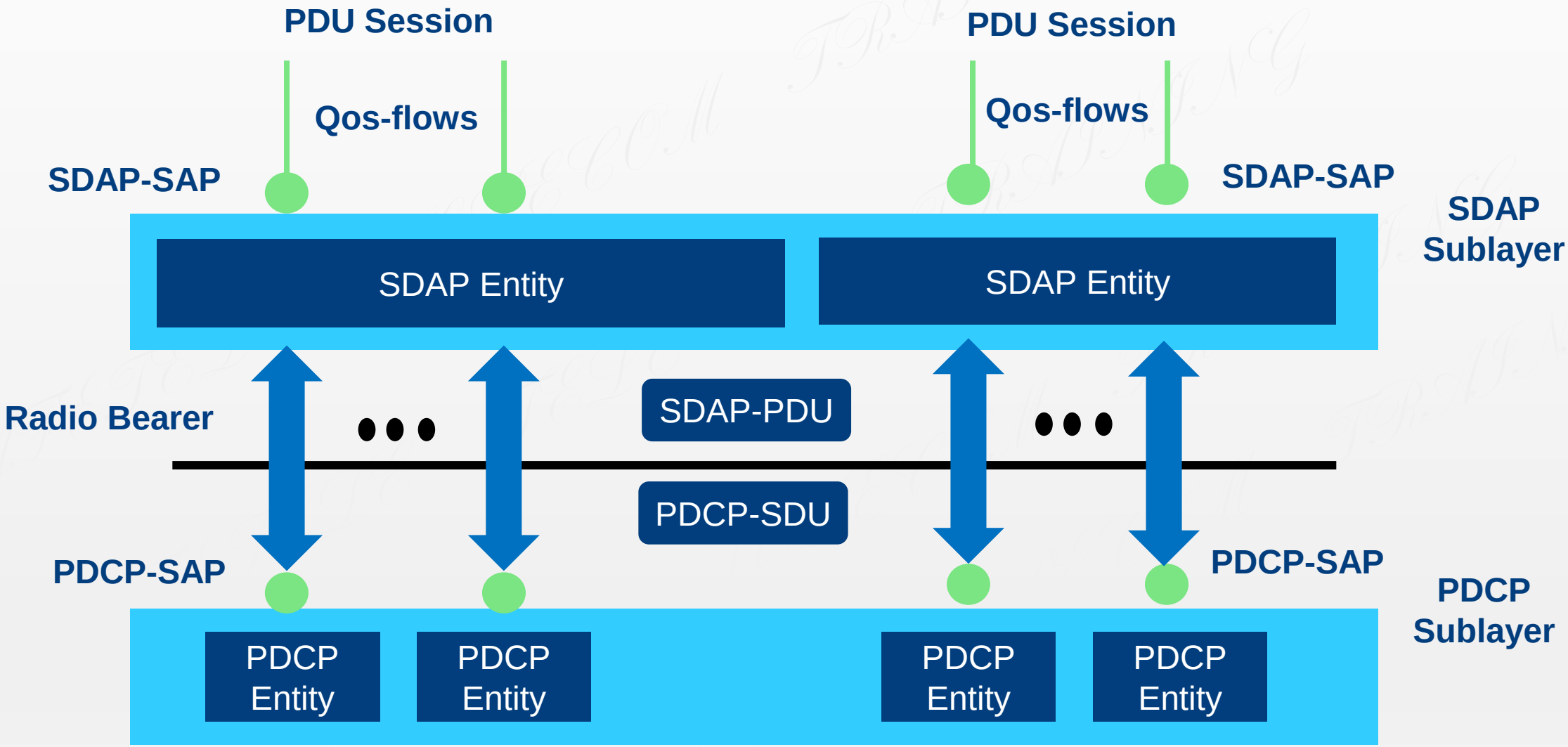
PDU SESSION MODIFICATION PENDING : This state signifies that modifications to the PDU session parameters or settings are being processed.

Followings are transition to other states:
To PDU SESSION ACTIVE: Triggered by PDU SESSION MODIFICATION COMMAND or PDU SESSION MODIFICATION REJECT
To PDU SESSION INACTIVE: Triggered by "PDU SESSION MODIFICATION REJECT

Service data Adaptation Protocol (SDAP)

SDAP sublayer, structure view

- PDU: Protocol Data Unit
- SDU: Service Data Unit
- SAP: Service Access Poin



SDAP Functions

❑Mapping between a QoS flow and a data radio bearer

- The QoS flow is the finest granularity of QoS differentiation in the PDU session
- A QoS Flow ID (QFI) is used to identify a QoS flow in the 5G system

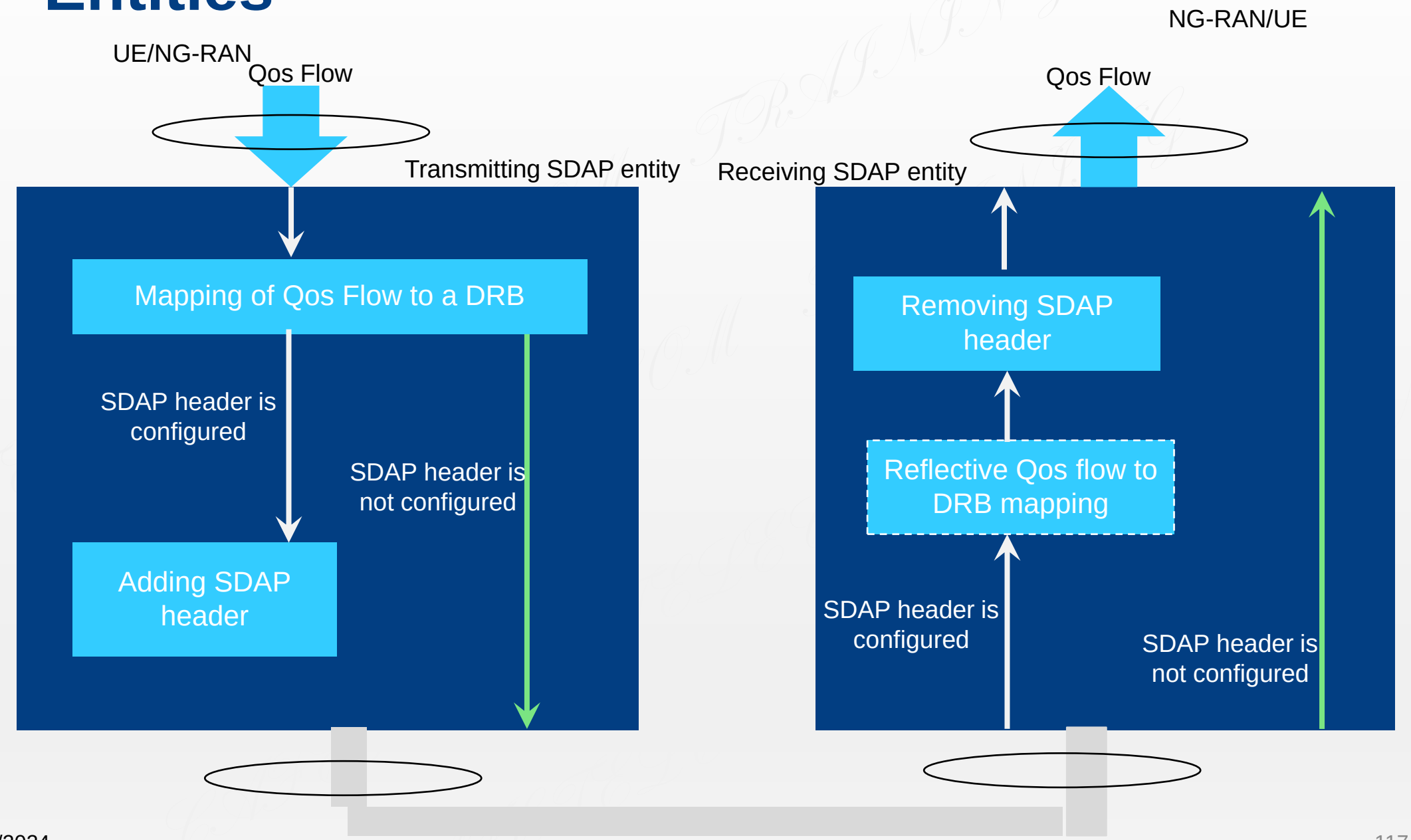
❑Marking QoS flow ID in both DL and UL packets

❖ Header include the “Flow ID” depending on network configuration

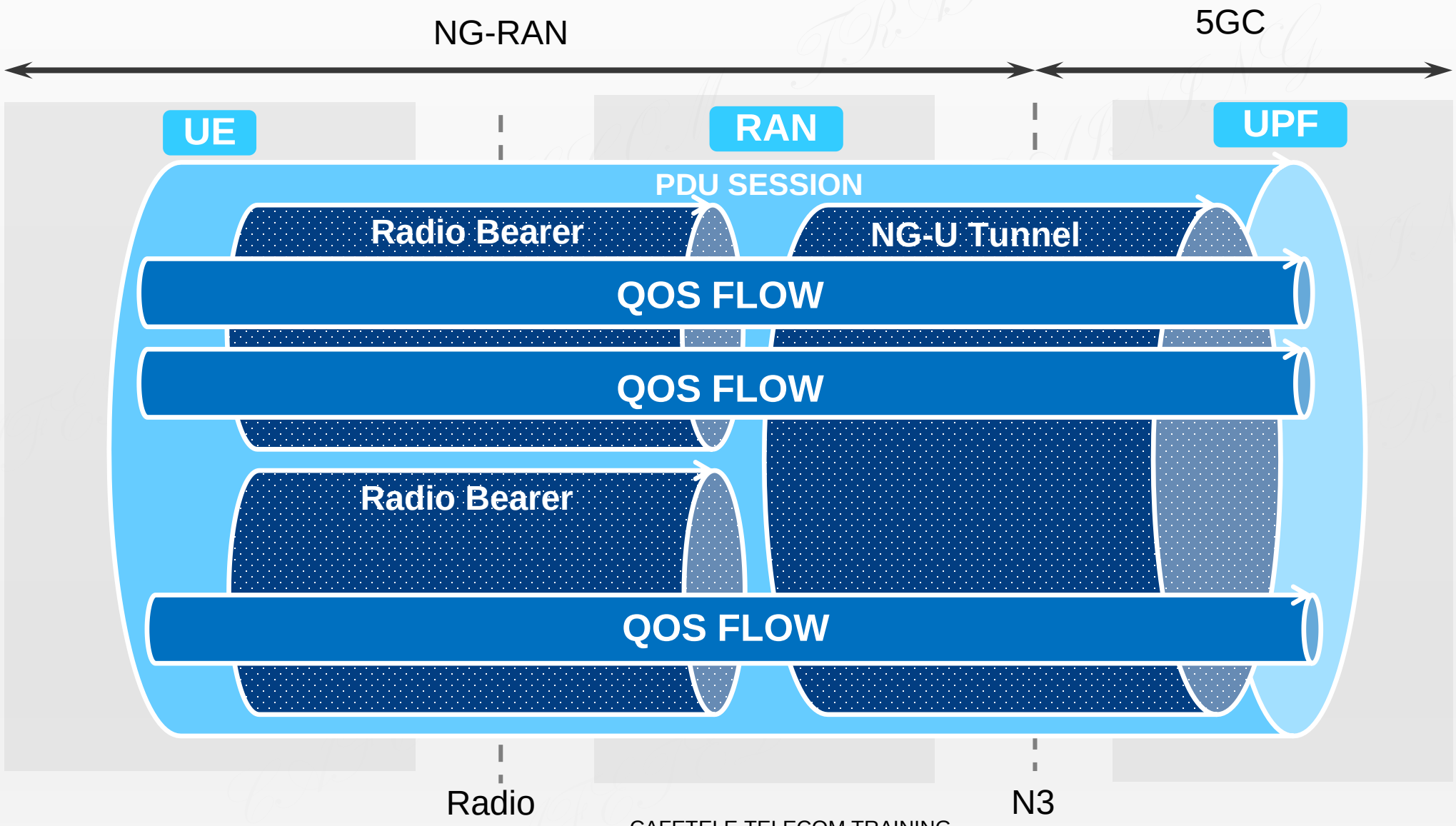
❖ 2-step mapping of IP flows

- NAS: IP flow QoS flow mapping
- AS: QoS flow DRB mapping

SDAP Entities



5G QOS Architecture: QOS FLOW



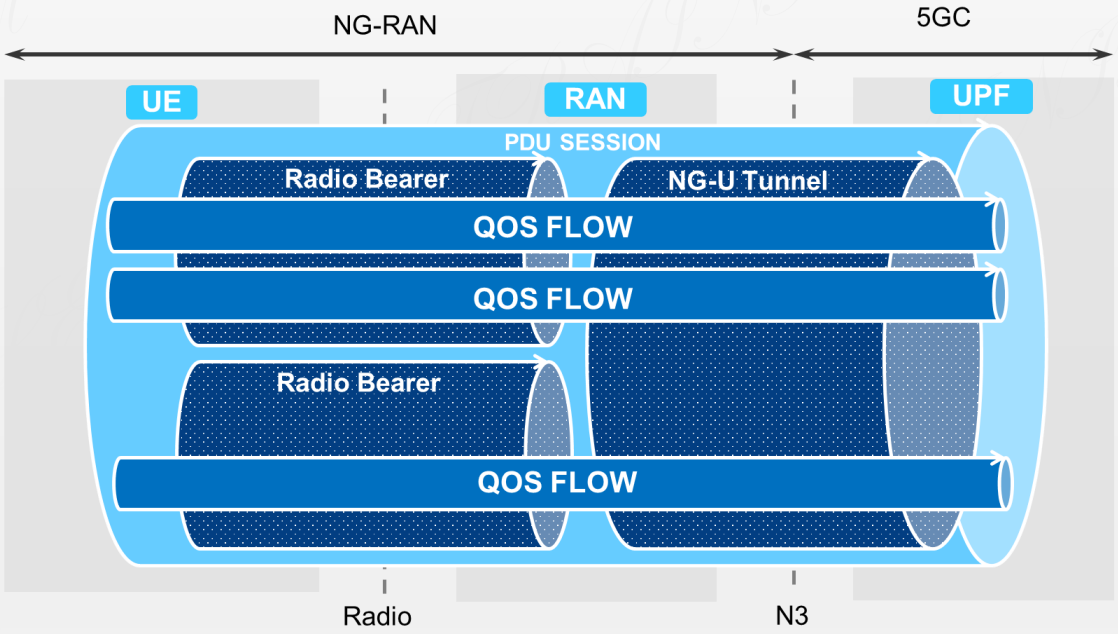
EPS bearer and QoS flow has the following differences

Item	4G	5G
Data path	EPS bearer	QoS flow
Identifier	EPS bearer ID (EBI)	QoS flow ID (QFI)
Category	•Default bearer •Dedicated bearer	•Default QoS flow •Dedicated QoS flow
Implementation on each interface	An EPS bearer needs to be mapped to different underlying bearers through different NEs and interfaces. The underlying bearers include radio bearers, S1 bearers, and S5/S8 bearers They are in a one-to-one relationship.	QoS flows involve only the bearers on the (R)AN side and do not actually have an end-to-end bearer. In addition, a PDU session uses a common NG-U tunnel, and a radio bearer maps to multiple QoS flows.
NE functions	Each network node is responsible for maintaining identifiers of underlying bearers and the binding relationships between them.	The UE and (R)AN are responsible for maintaining data radio bearer (DRB) IDs as well as the binding relationships between DRB IDs and QFIs.

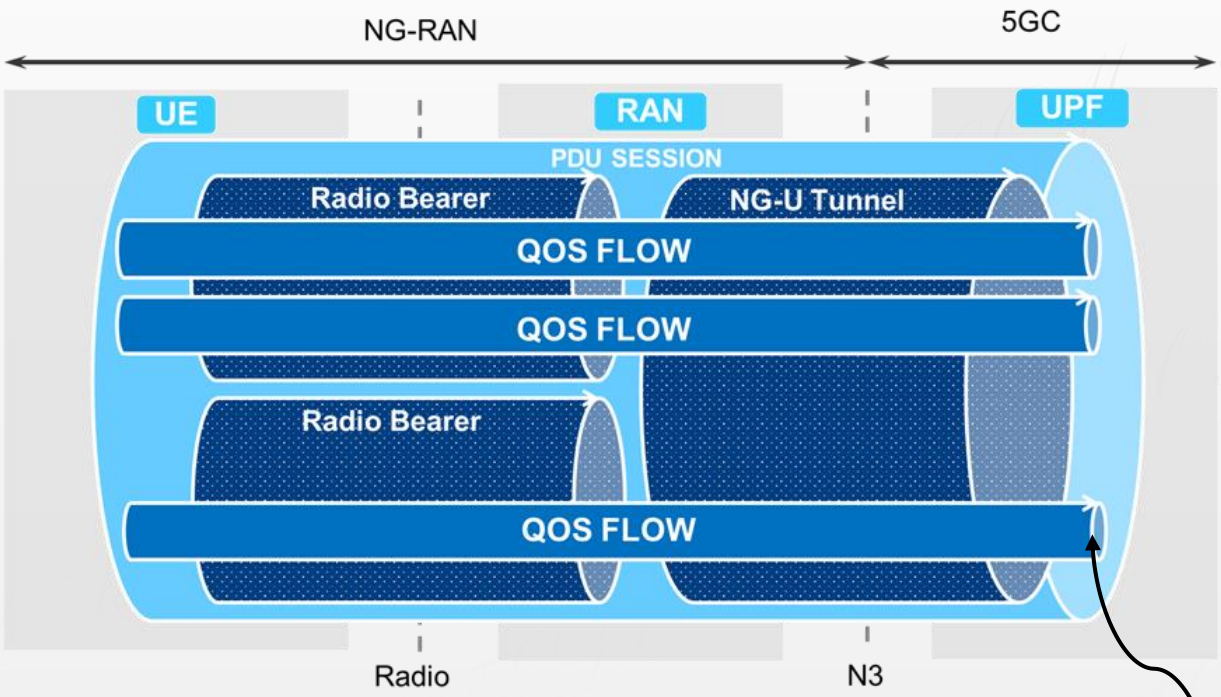
5G QOS Framework

- QoS Model
  - Supports QoS flow based framework
  - Supports both QoS flows of guaranteed flow bit rate and non-guaranteed flow bit rate
  - Also supports reflective QoS
    - A QoS rule for UL is derived from received DL traffic
    - UL packets get the same QoS marking as the reflected DL packet

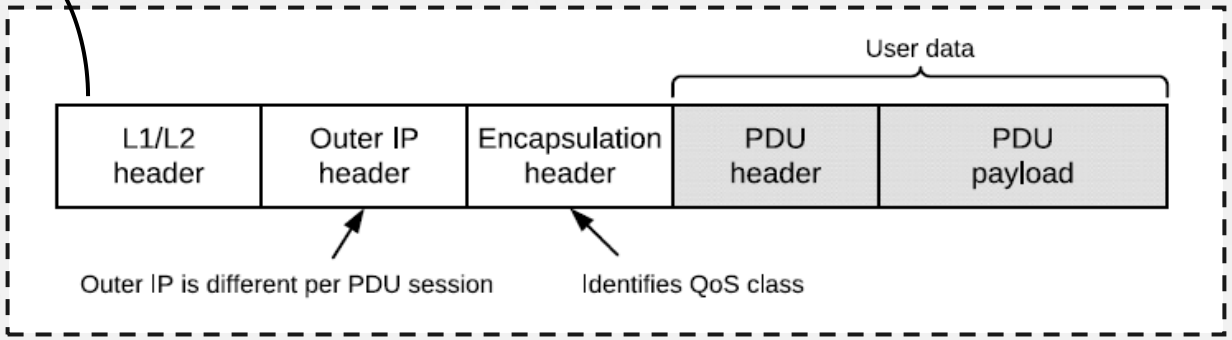
- Architecture
  - 1UE = 1+ PDU sessions
  - 1 PDU Session = 1+ DRBs(Data Radio Bearers)
  - 1 DRB = 1+ QoS Flows
  - UL/DL packet to QoS Flow mapping in the UE & UPF
  - QoS Flows to DRBs mapping in the gNB



5G QoS Overview



- A QoS flow is the finest granularity of QoS differentiation in a PDU session
- One PDU session can carry one or several QoS flows
- A Radio Bearer can carry one or several QoS flows



Standardized 5QI to QoS characteristics mapping (GBR)

5QI Value	Resource Type	Default Priority Level	Packet Delay Budget	Packet Error Rate	Default Averaging Window	Example Services
1	GBR NOTE 1	20	100 ms	10^{-2}	2000 ms	Conversational Voice
2		40	150 ms	10^{-3}	2000 ms	Conversational Video (Live Streaming)
3		30	50 ms	10^{-3}	2000 ms	Real Time Gaming, V2X messages Electricity distribution – medium voltage, Process automation - monitoring
4		50	300 ms	10^{-6}	2000 ms	Non-Conversational Video (Buffered Streaming)
65		7	75 ms	10^{-2}	2000 ms	Mission Critical user plane Push To Talk voice (e.g., MCPTT)
66		20	100 ms	10^{-2}	2000 ms	Non-Mission-Critical user plane Push To Talk voice
67		15	100 ms	10^{-3}	2000 ms	Mission Critical Video user plane
75		25	50 ms	10^{-2}	2000 ms	V2X messages

5QI: 5G QoS Indicator **QFI**: QoS Flow ID **GBR**: Guaranteed Bit Rate **V2X**: Vehicle to anything

Standardized 5QI to QoS characteristics mapping (Non-GBR)

5QI Value	Resource Type	Priority Level	Packet Delay Budget	Packet Error Rate	Example Services
5	Non-GBR	10	100 ms	10^{-6}	IMS Signalling
6	NOTE 1	60	300 ms	10^{-6}	Video (Buffered Streaming) TCP-based (e.g., www, e-mail, chat, ftp, p2p file sharing, progressive video, etc.)
7		70	100 ms	10^{-3}	Voice, Video (Live Streaming) Interactive Gaming
8		80	300 ms	10^{-6}	Video (Buffered Streaming) TCP-based (e.g., www, e-mail, chat, ftp, p2p file sharing, progressive video, etc.)
9		90			Best Effort (Internet)
69		5	60 ms	10^{-6}	Mission Critical delay sensitive signalling (e.g., MC-PTT signalling)
70		55	200 ms	10^{-6}	Mission Critical Data (e.g. example services are the same as QCI 6/8/9)
79		65	50 ms	10^{-2}	V2X messages
80		68	10 ms	10^{-6}	Low Latency eMBB applications Augmented Reality

5QI: 5G QoS Indicator **QFI**: QoS Flow ID **GBR**: Guaranteed Bit Rate **V2X**: Vehicle to anything

Standardized 5QI to QoS characteristics mapping (Delay Critical GBR)

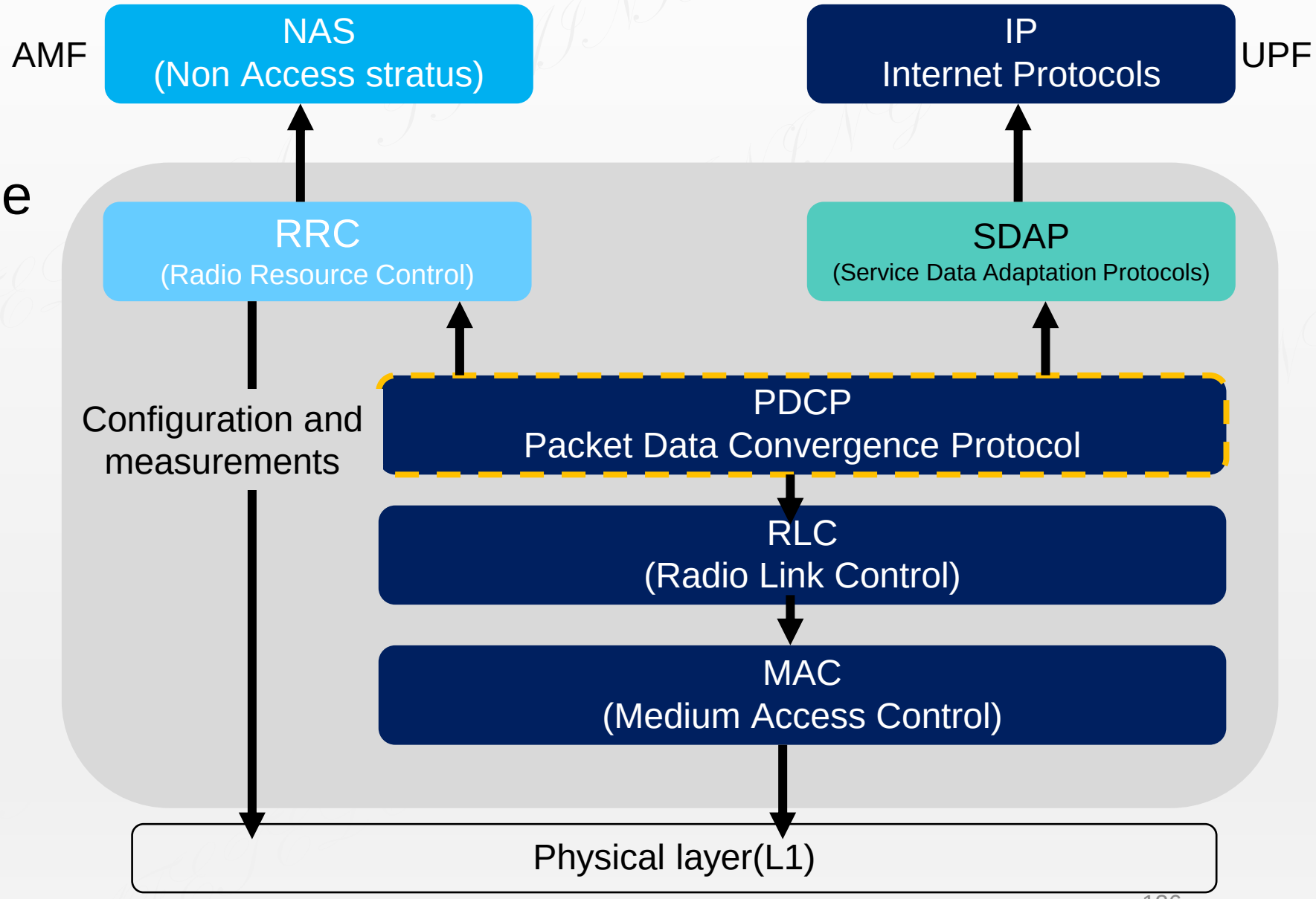
5QI Value	Resource Type	Priority Level	Packet Delay Budget	Packet Error Rate	Default Maximum Data Burst Volume (NOTE 2)	Default Averaging Window	Example Services
81	Delay Critical GBR	11	5 ms	10^{-5}	160 B	2000 ms	**Remote control (see TS 22.261)**
82		12	10 ms NOTE 5	10^{-5}	320 B	2000 ms	**Intelligent transport systems**
83		13	20 ms	10^{-5}	640 B	2000 ms	**Intelligent Transport Systems**
84		19	10 ms	10^{-4}	255 B	2000 ms	**Discrete Automation**
85		22	10 ms	10^{-4}	1358 B NOTE 3	2000 ms	**Discrete Automation**

5QI: 5G QoS Indicator **QFI**: QoS Flow ID **GBR**: Guaranteed Bit Rate **V2X**: Vehicle to anything

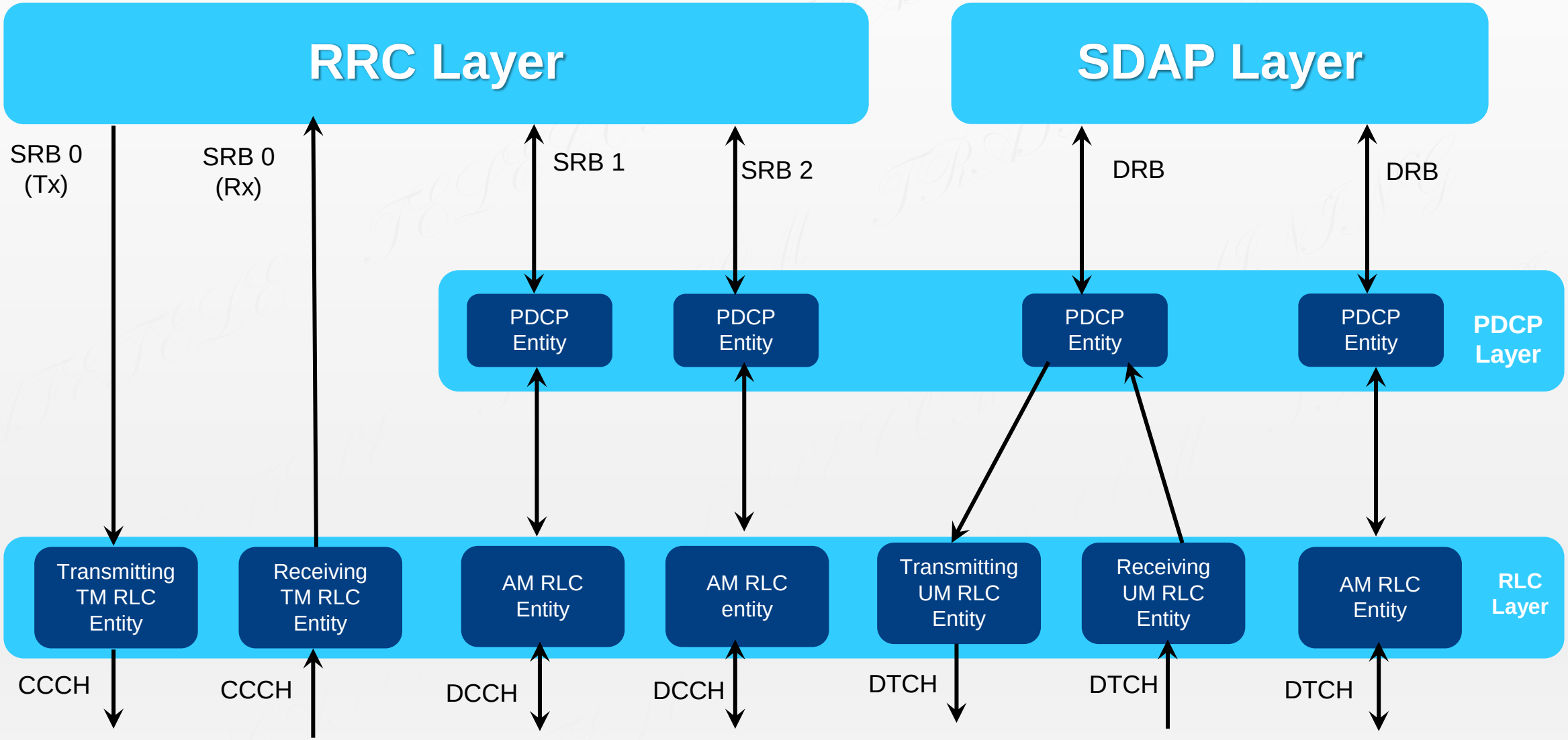
Packet Data Convergence Protocol (PDCP)

Packet Data Convergence Protocol

- Transfer of user plane data
- Transfer of control plane data
- IP Header compression
- Integrity protection(CP)
- Ciphering(UP & CP)



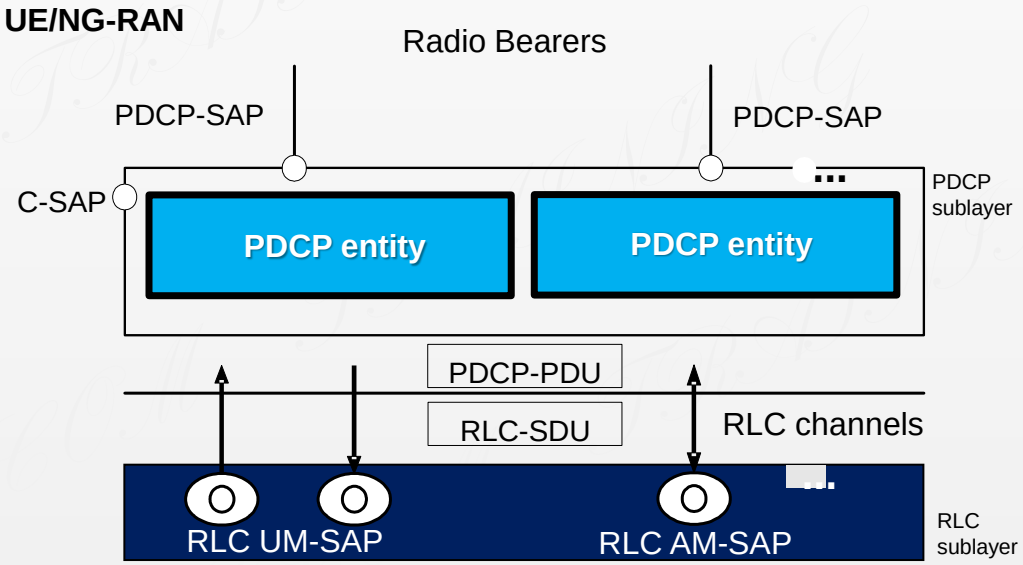
PDCP Layer Serving DRB,SRB



Packet Data Convergence Protocol

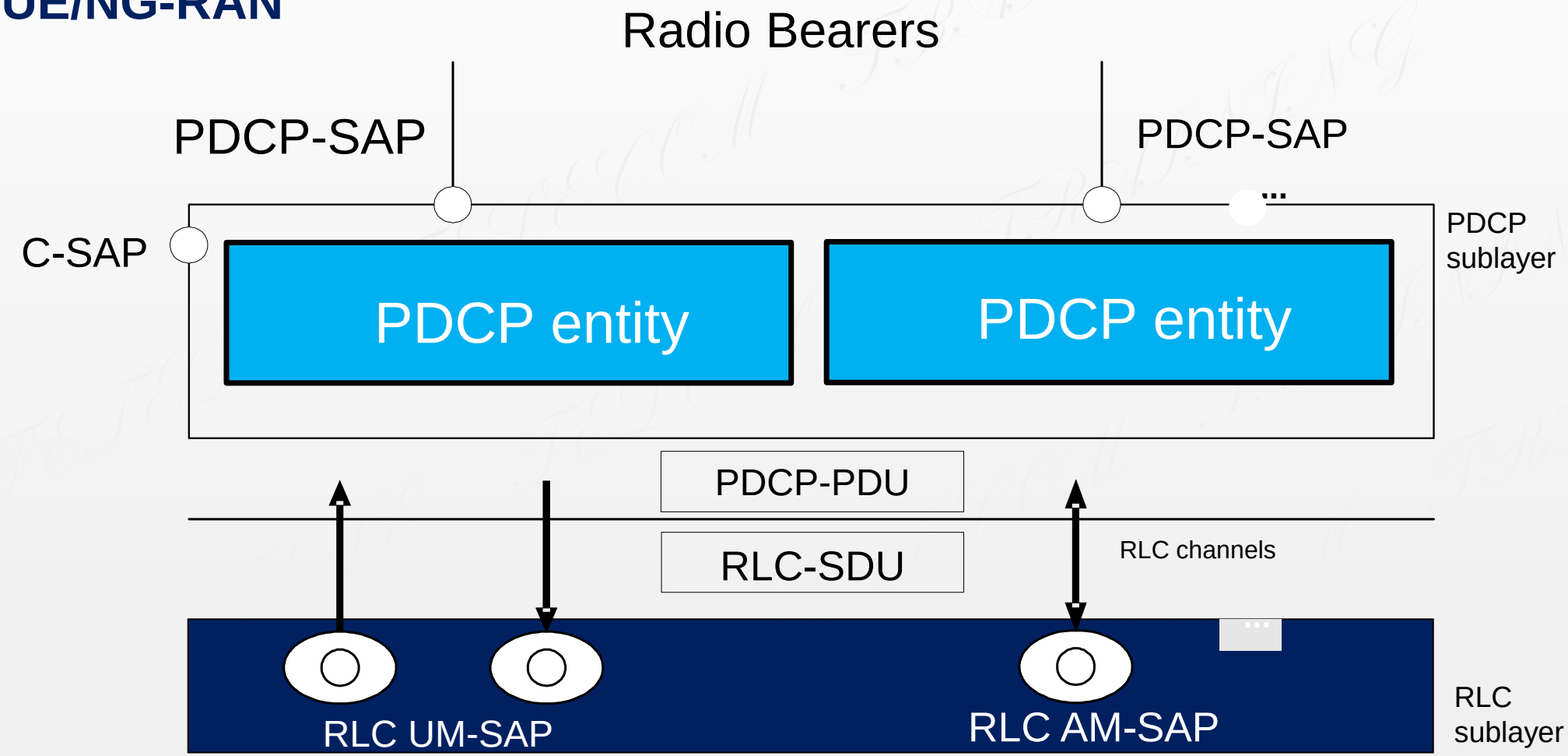
❖PDCP Functions

- Transfer of data (user plane or control plane)
- Maintenance of PDCP SNs
- Header compression and decompression using the ROHC protocol
- Ciphering and deciphering
- Integrity protection and integrity verification
- Timer based SDU discard
- For split bearers, routing
- Duplication
- Reordering and in-order delivery
- Out-of-order delivery
- Duplicate discarding



3GPP TS 38.323

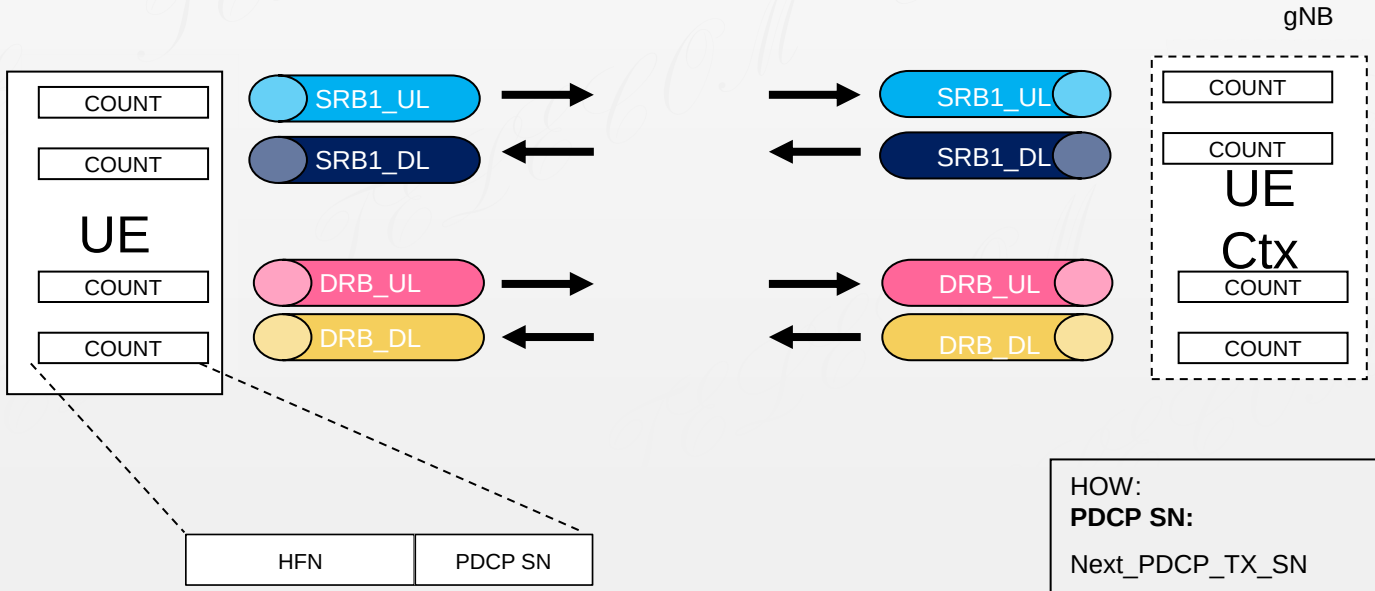
UE/NG-RAN



PDCP layer, structure view

Sequence Numbering

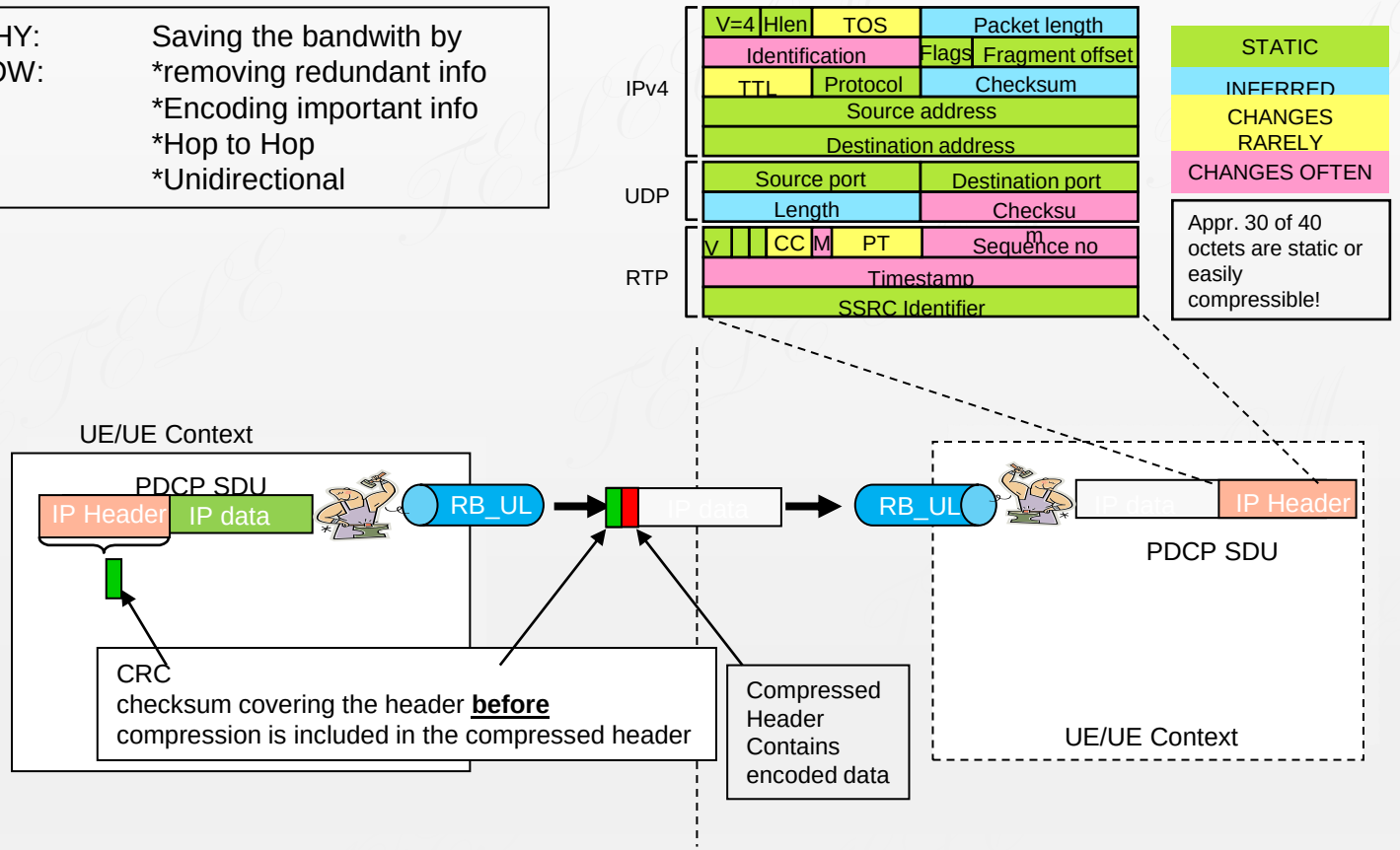
WHY:
* Reordering
* Duplicate detection
* Integrity protection
* Ciphering



HOW:
PDCP SN:
Next_PDCP_TX_SN
TX_HFN
COUNT

Header Compression

WHY: Saving the bandwith by
HOW: *removing redundant info
*Encoding important info
*Hop to Hop
*Unidirectional



Supported profiles	
Profile Identifier	**Usage**
0x0000	No compression
0x0001	RTP/UDP/IP
0x0002	UDP/IP
0x0003	ESP/IP
0x0004	IP
0x0006	TCP/IP
0x0101	RTP/UDP/IP
0x0102	UDP/IP
0x0103	ESP/IP
0x0104	IP

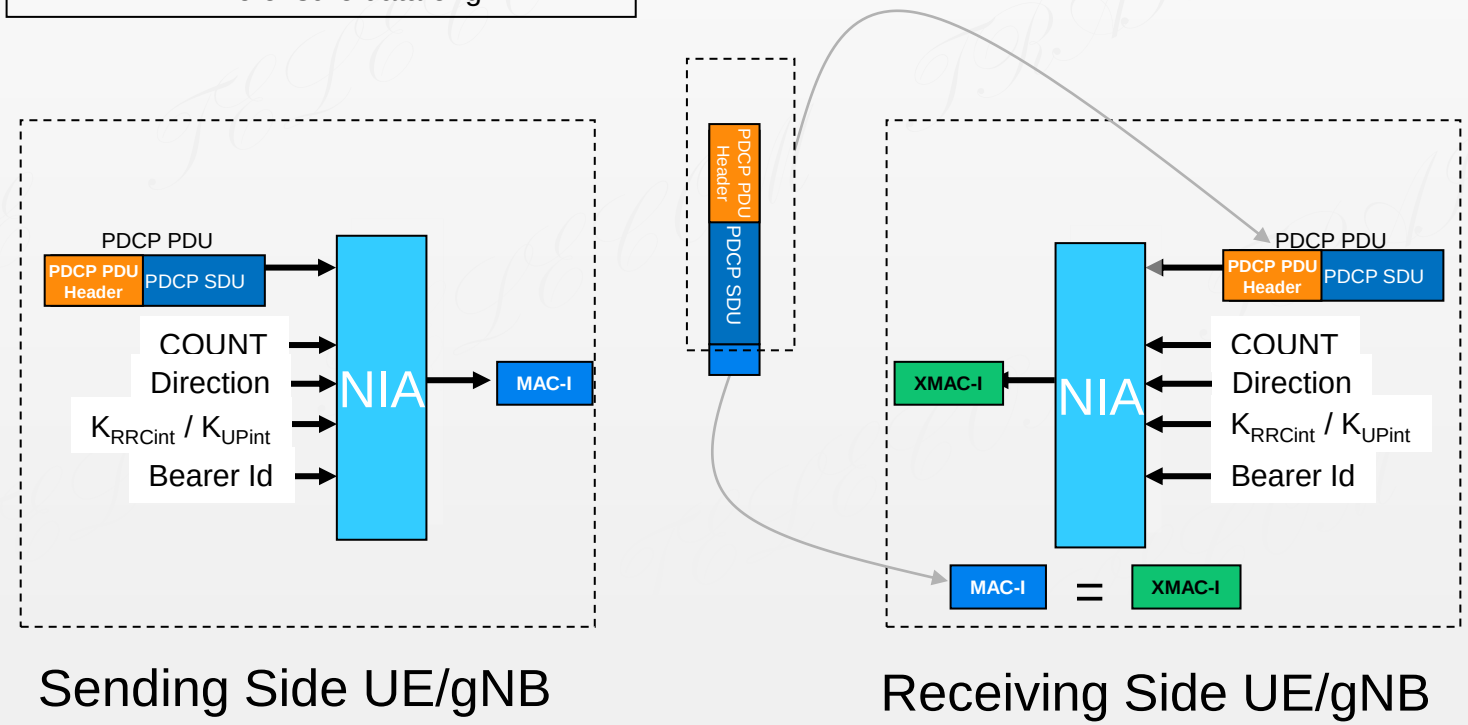
ROHC is only applied to IP packets
Not to SDAP header

Thus, PDCP layer needs to know:
If SDAP layer adds the SDAP header
Length of SDAP header

Integrity Protection

NIA0 – Null Integrity Protection
NIA1 – SNOW 3G based
NIA2 – AES based
NIA3 – ZUC based

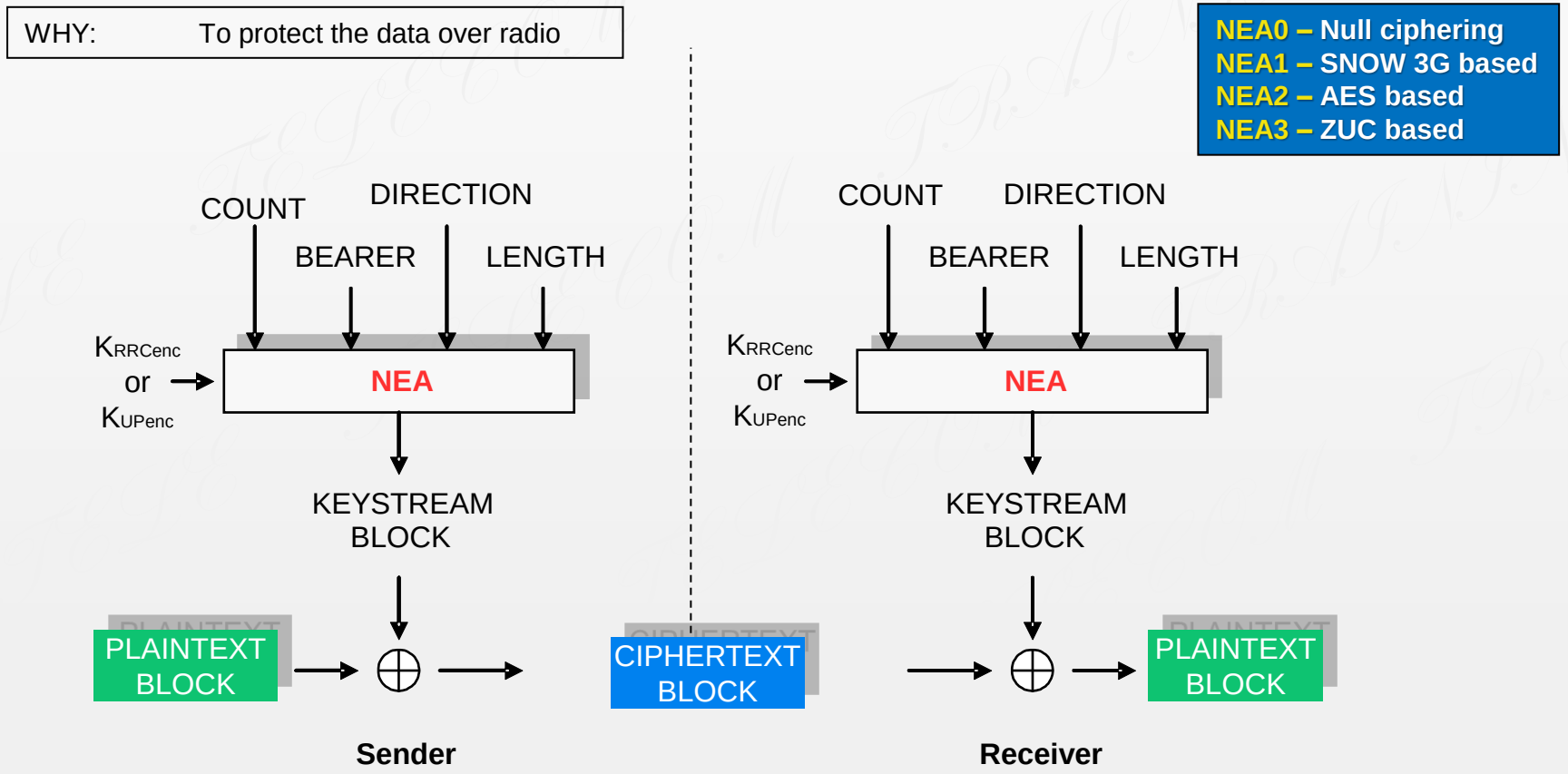
WHY: To ensure data origin



Sending Side UE/gNB

Receiving Side UE/gNB

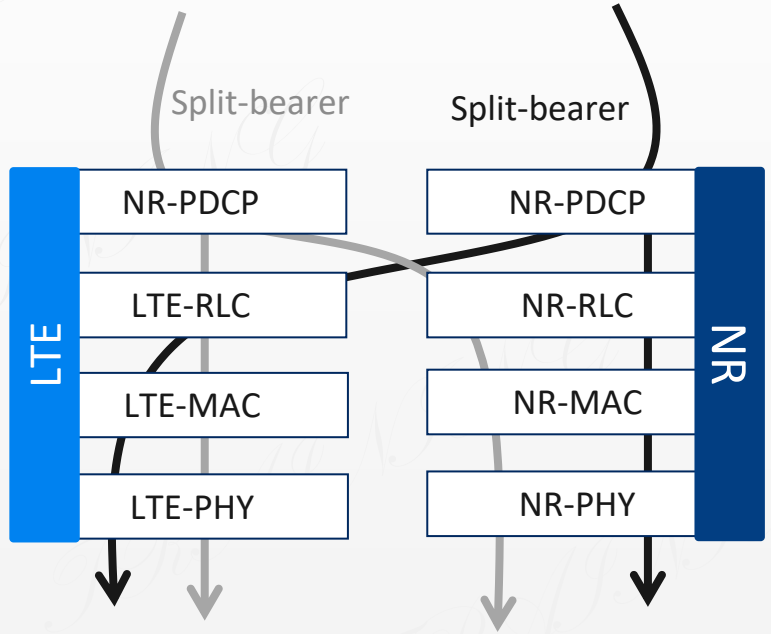
Ciphering


WHY: To protect the data over radio
NEA0 – Null ciphering
NEA1 – SNOW 3G based
NEA2 – AES based
NEA3 – ZUC based
COUNT
DIRECTION
BEARER
LENGTH
KRRCenc
or
KUPenc
NEA
KEYSTREAM BLOCK
PLAINTEXT BLOCK
CIPHERTEXT BLOCK
PLAINTEXT BLOCK
Sender
Receiver

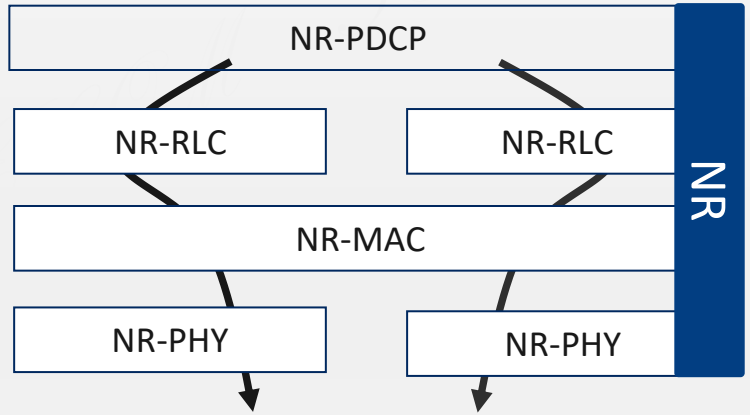
PDCP Data Duplication

- Secondary RLC entity / logical channel is added to the DRB
- Increases reliability and reduces latency
- Configured by RRC
- If Packet Duplication is configured:
  - Packet duplication can be activated or deactivated dynamically via MAC Control Elements (CE) for DRBs
  - Duplication is always active for SRB
- Duplicate discard based on RLC AM on transmitting side

Dual Connectivity



Carrier Aggregation



Supported for bearers mapped on RLC AM and UM